CANONICAL SUBGROUPS OF BARSOTTI-TATE GROUPS

YICHAO TIAN

Abstract. Let S be the spectrum of a complete discrete valuation ring with fraction field of characteristic 0 and perfect residue field of characteristic $p \geq 3$. Let G be a truncated Barsotti-Tate group of level 1 over S. If "G is not too supersingular", a condition that will be explicitly expressed in terms of the valuation of a certain determinant, we prove that we can canonically lift the kernel of the Frobenius endomorphism of its special fibre to a subgroup scheme of G, finite and flat over S. We call it the canonical subgroup of G.

1. Introduction

1.1. Let $\mathcal{O}_K$ be a complete discrete valuation ring with fraction field K of characteristic 0 and perfect residue field k of characteristic $p > 0$. We put $S = \mathrm{Spec}(\mathcal{O}_K)$ and denote by s (resp. η) its closed (resp. generic) point. Let G be a truncated Barsotti-Tate group of level 1 over S. If G_s is ordinary, the kernel of its Frobenius endomorphism is a multiplicative group scheme and can be uniquely lifted to a closed subgroup scheme of G, finite and flat over S. If we do not assume G_s ordinary but only that "G is not too supersingular", a condition that will be explicitly expressed in terms of the valuation of a certain determinant, we will prove that we can still canonically lift the kernel of the Frobenius endomorphism of G_s to a subgroup scheme of G, finite and flat over S. We call it *the canonical subgroup* of G. Equivalently, under the same condition, we will prove that the Frobenius endomorphism of G_s can be canonically lifted to an isogeny of truncated Barsotti-Tate groups over S. This problem was first raised by Lubin in 1967 and solved by himself for 1-parameter formal groups [16]. A slightly weaker question was asked by Dwork in 1969 for abelian schemes and answered also by him for elliptic curves [9]: namely, could we extend the construction of the canonical subgroup in the ordinary case to a "tubular neighborhood" (without requiring that it lifts the kernel of the Frobenius)? The dimension one case played a fundamental role in the pioneering work of Katz on p-adic modular forms [14]. For higher dimensional abelian schemes, Dwork's conjecture was first solved by Abbes and Mokrane [1]; our approach is a generalization of their results. Later, there have been other proofs, always for abelian schemes, by Andreatta and Gasbarri [3], Kisin and Lai [15] and Conrad [7].

1.2. For an S-scheme X, we denote by X_1 its reduction modulo p. The valuation v_p of K, normalized by $v_p(p) = 1$, induces a truncated valuation $\mathcal{O}_{S_1} \backslash \{0\} \to \mathbb{Q} \cap [0, 1)$. Let G be a truncated Barsotti-Tate group of level 1 and height h over S, $G^\vee$ be its Cartier dual, and d be the dimension of the Lie algebra of G_s over k. The Lie algebra $\mathrm{Lie}(G_1^\vee)$ of $G_1^\vee$ is a free $\mathcal{O}_{S_1}$-module of rank $d^* = h - d$, canonically isomorphic to $\mathrm{Hom}_{(S_1)_{\mathrm{fppf}}}(G_1, \mathbb{G}_a)$ ([12] 2.1). The Frobenius homomorphism of $\mathbb{G}_a$ over S_1 induces an endomorphism F of $\mathrm{Lie}(G_1^\vee)$, which is semi-linear with respect to the Frobenius homomorphism of $\mathcal{O}_{S_1}$. We define the Hodge height (3.11) of $\mathrm{Lie}(G_1^\vee)$ to be the truncated valuation of the determinant of a matrix of F. This invariant measures the ordinarity of G.

1.3. Following [1], we construct the canonical subgroup of a truncated Barsotti-Tate group over S by the ramification theory of Abbes and Saito [2]. Let G be a commutative finite and flat group scheme over S. In [1], the authors defined a canonical exhaustive decreasing filtration $(G^a, a \in \mathbb{Q}_{\geq 0})$ by finite, flat and closed subgroup schemes of G. For a real number $a \geq 0$, we put $G^{a+} = \cup_{b>a} G^b$, where b runs over rational numbers.

Theorem 1.4. *Assume that $p \geq 3$, and let e be the absolute ramification index of K and $j = e/(p-1)$. Let G be a truncated Barsotti-Tate group of level 1 over S, d be the dimension of the Lie algebra of G_s over k. Assume that the Hodge height of $\mathrm{Lie}(G_1^\vee)$ is strictly smaller than $1/p$. Then,*

(i) *the subgroup scheme G^{j+} of G is locally free of rank p^d over S;*
(ii) *the special fiber of G^{j+} is the kernel of the Frobenius endomorphism of G_s.*

1.5. Statement (i) was proved by Abbes and Mokrane [1] for the kernel of multiplication by p of an abelian scheme over S. We extend their result to truncated Barsotti-Tate groups by using a theorem of Raynaud to embed G into an abelian scheme over S. To prove statement (ii), which we call *"the lifting property of the canonical subgroup"*, we give a new description of the canonical filtration of a finite, flat and commutative group scheme over S killed by p in terms of *congruence groups*. Let $\overline{K}$ be an algebraic closure of the fraction field of S, $\mathcal{O}_{\overline{K}}$ be the integral closure of $\mathcal{O}_K$ in $\overline{K}$. Put $\overline{S} = \mathrm{Spec}(\mathcal{O}_{\overline{K}})$. For every $\lambda \in \mathcal{O}_{\overline{K}}$ with $0 \leq v_p(\lambda) \leq 1/(p-1)$, Sekiguchi, Oort and Suwa [20] introduced a finite and flat group scheme G_λ of order p over $\overline{S}$ (see (7.1)); following Raynaud, we call it the congruence group of level λ. If $v_p(\lambda) = 0$, G_λ is isomorphic to the multiplicative group scheme $\mu_p = \mathrm{Spec}(\mathcal{O}_{\overline{K}}[X]/(X^p - 1))$ over $\overline{S}$; and if $v_p(\lambda) = 1/(p-1)$, G_λ is isomorphic to the the constant étale group scheme $\mathbb{F}_p$. For general $\lambda \in \mathcal{O}_{\overline{K}}$ with $0 \leq \lambda \leq 1/(p-1)$, there is a canonical $\overline{S}$-homomorphism $\theta_\lambda : G_\lambda \to \mu_p$, such that $\theta \otimes \overline{K}$ is an isomorphism. For a finite, flat and commutative group scheme G over S killed by p, θ_λ induces a homomorphism

$$\theta_\lambda(G)\colon\ \mathrm{Hom}_{\overline{S}}(G, G_\lambda) \to G^\vee(\overline{K}) = \mathrm{Hom}_{\overline{S}}(G, \mu_p).$$

We prove that it is injective, and its image depends only on the valuation $a = v_p(\lambda)$; we denote it by $G^\vee(\overline{K})^{[ea]}$, where e is the absolute ramification index of K (the multiplication by e will be justified later). Moreover, we get a decreasing exhaustive filtration $(G^\vee(\overline{K})^{[a]}, a \in \mathbb{Q} \cap [0, \frac{e}{p-1}])$.

Theorem 1.6. *Let G be a finite, flat and commutative group scheme over S killed by p. Under the canonical perfect pairing*

$$G(\overline{K}) \times G^\vee(\overline{K}) \to \mu_p(\overline{K}),$$

we have for any rational number $a \in \mathbb{Q}_{\geq 0}$,

$$G^{a+}(\overline{K})^\perp = \begin{cases} G^\vee(\overline{K})^{[\frac{e}{p-1} - \frac{a}{p}]}, & \text{if} \quad 0 \leq a \leq \frac{ep}{p-1}, \\ G^\vee(\overline{K}), & \text{if} \quad a > \frac{ep}{p-1}. \end{cases}$$

Andreatta and Gasbarri [3] have used congruence groups to prove the existence of the canonical subgroup for abelian schemes. This theorem explains the relation between the approach via the ramification theory of [1] and this paper, and the approach of [3].

1.7. This article is organized as follows. For the convenience of the reader, we recall in section 2 the theory of ramification of group schemes over a complete discrete valuation ring, developed in [2] and [1]. Section 3 is a summary of the results in [1] on the canonical subgroup of an abelian scheme over S. Section 4 consists of some preliminary results on the fppf cohomology of abelian schemes. In section 5, we define the Bloch-Kato filtration for a finite, flat and commutative group scheme over S killed by p. Using this filtration, we prove Theorem 1.4(i) in section 6. Section 7

is dedicated to the proof of Theorem 1.6. Finally in section 8, we complete the proof of Theorem 1.4(ii).

1.8. This article is a part of the author's thesis at Université Paris 13. The author would like to express his great gratitude to his thesis advisor Professor A. Abbes for leading him to this problem and for his helpful comments on earlier versions of this work. The author thanks Professors W. Messing and M. Raynaud for their help. He is also grateful to the referee for his careful reading and very valuable comments.

1.9. **Notation.** In this article, $\mathcal{O}_K$ denotes a complete discrete valuation ring with fraction field K of characteristic 0, and residue field k of characteristic $p>0$. Except in Section **2**, we will assume that k is perfect. Let $\overline{K}$ be an algebraic closure of K, $\mathcal{G}_K=\mathrm{Gal}(\overline{K}/K)$ be the Galois group of $\overline{K}$ over K, $\mathcal{O}_{\overline{K}}$ be the integral closure of $\mathcal{O}_K$ in $\overline{K}$, $\mathfrak{m}_{\overline{K}}$ the maximal ideal of $\mathcal{O}_{\overline{K}}$, and $\overline{k}$ be the residue field of $\mathcal{O}_{\overline{K}}$.

We put $S=\mathrm{Spec}(\mathcal{O}_K)$, $\overline{S}=\mathrm{Spec}(\mathcal{O}_{\overline{K}})$, and denote by s and η (*resp.* $\overline{s}$ and $\overline{\eta}$) the closed and generic point of S (*resp.* of $\overline{S}$) respectively.

We fix a uniformizer π of $\mathcal{O}_K$. We will use two valuations v and v_p on $\mathcal{O}_K$, normalized respectively by $v(\pi)=1$ and $v_p(p)=1$; so we have $v=ev_p$, where e is the absolute ramification index of K. The valuations v and v_p extend uniquely to $\overline{K}$; we denote the extensions also by v and v_p. For a rational number $a\geq 0$, we put $\mathfrak{m}_a=\{x\in\overline{K}; v_p(x)\geq a\}$ and $\overline{S}_a=\mathrm{Spec}(\mathcal{O}_{\overline{K}}/\mathfrak{m}_a)$. If X is a scheme over S, we will denote respectively by $\overline{X}$, $X_{\overline{s}}$ and $\overline{X}_a$ the schemes obtained by base change of X to $\overline{S}$, $\overline{s}$ and $\overline{S}_a$.

If G is a commutative, finite and flat group scheme over S, we will denote by $G^\vee$ its Cartier dual. For an abelian scheme A over S, $A^\vee$ will denote the dual abelian scheme, and ${}_pA$ the kernel of multiplication by p, which is a finite and flat group scheme over S.

2. Ramification theory of finite flat group schemes over S

2.1. We begin by recalling the main construction of [2]. Let A be a finite and flat $\mathcal{O}_K$-algebra. We fix a finite presentation of A over $\mathcal{O}_K$

$$0\to I\to\mathcal{O}_K[x_1,\cdots,x_n]\to A\to 0,$$

or equivalently, an S-closed immersion of $i\colon \mathrm{Spec}(A)\to\mathbb{A}^n_S$. For a rational number $a>0$, let X^a be the tubular neighborhood of i of thickening a ([2] Section 3, [1] 2.1). It is an affinoid subdomain of the n-dimensional closed unit disc over K given by

$$X^a(\overline{K})=\{(x_1,\cdots,x_n)\in\mathcal{O}^n_{\overline{K}}|\ \ v(f(x_1,\cdots,x_n))\geq a,\quad \forall f\in I\}.$$

Let $\pi_0(X^a_{\overline{K}})$ be the set of geometric connected components of X^a. It is a finite $\mathcal{G}_K$-set that does not depend on the choice of the presentation ([2] Lemma 3.1). We put

$$\mathcal{F}^a(A)=\pi_0(X^a_{\overline{K}}). \tag{2.1.1}$$

For two rational numbers $b\geq a>0$, X^b is an affinoid sub-domain of X^a. So there is a natural transition map $\mathcal{F}^b(A)\to\mathcal{F}^a(A)$.

2.2. We denote by $\mathrm{AFP}_{\mathcal{O}_K}$ the category of finite flat $\mathcal{O}_K$-algebras, and by $\mathcal{G}_K$-Ens the category of finite sets with a continuous action of $\mathcal{G}_K$. Let

$$\begin{array}{rcl}\mathcal{F}\colon \mathrm{AFP}^\circ_{\mathcal{O}_K} & \to & \mathcal{G}_K\text{-Ens}\\ A & \mapsto & \mathrm{Spec}(A)(\overline{K})\end{array}$$

be the functor of geometric points. For $a \in \mathbb{Q}_{>0}$, (2.1.1) gives rise to a functor

$$\mathcal{F}^a : \mathrm{AFP}^{\circ}_{\mathcal{O}_K} \to \mathcal{G}_K\text{-Ens}.$$

For $b \geq a \geq 0$, we have morphisms of functors $\phi^a : \mathcal{F} \to \mathcal{F}^a$ and $\phi^a_b : \mathcal{F}^b \to \mathcal{F}^a$, satisfying the relations $\phi^a = \phi^b \circ \phi^a_b$ and $\phi^a_c = \phi^a_b \circ \phi^b_c$ for $c \geq b \geq a \geq 0$. To stress the dependence on K, we will denote $\mathcal{F}$ (*resp.* $\mathcal{F}^a$) by $\mathcal{F}_K$ (*resp.* $\mathcal{F}^a_K$). These functors behave well only for finite, flat and relative complete intersection algebras over $\mathcal{O}_K$ (EGA IV 19.3.6). We refer to [2] Propositions 6.2 and 6.4 for their main properties.

Lemma 2.3 ([1] Lemme 2.1.5)**.** *Let K'/K be an extension (not necessarily finite) of complete discrete valuation fields with ramification index $e_{K'/K}$. Let A be a finite, flat and relative complete intersection algebra over $\mathcal{O}_K$. Then we have a canonical isomorphism $\mathcal{F}^{ae_{K'/K}}_{K'}(A') \simeq \mathcal{F}^a_K(A)$ for all $a \in \mathbb{Q}_{>0}$.*

2.4. Abbes and Saito show that the projective system of functors $(\mathcal{F}^a, \mathcal{F} \to \mathcal{F}^a)_{a\in\mathbb{Q}_{\geq 0}}$ gives rise to an exhaustive decreasing filtration $(\mathcal{G}^a_K, a \in \mathbb{Q}_{\geq 0})$ of the group $\mathcal{G}_K$, called the *ramification filtration* ([2] Proposition 3.3). Concretely, if L is a finite Galois extension of K contained in $\overline{K}$, $\mathrm{Gal}(L/K)$ is the Galois group of L/K, then the quotient filtration $(\mathrm{Gal}(L/K)^a)_{a\in\mathbb{Q}_{\geq 0}}$ induced by $(\mathcal{G}^a_K)_{a\in\mathbb{Q}_{\geq 0}}$ is determined by the following canonical isomorphisms

$$\mathcal{F}^a(L) \simeq \mathrm{Gal}(L/K)/\,\mathrm{Gal}(L/K)^a.$$

For a real number $a \geq 0$, we put $\mathcal{G}^{a+}_K = \overline{\cup_{b>a}\mathcal{G}^b_K}$, and if $a > 0$ $\mathcal{G}^{a-}_K = \cap_{b<a}\mathcal{G}^b_K$, where b runs over rational numbers. Then $\mathcal{G}^{0+}_K$ is the inertia subgroup of $\mathcal{G}_K$ ([2] Proposition 3.7).

2.5. We recall the definition of the canonical filtration of a finite and flat group schemes over S, following [1]. Let Gr_S be the category of finite, flat and commutative group schemes over S. Let G be an object of Gr_S and $a \in \mathbb{Q}_{\geq 0}$. Then there is a natural group structure on $\mathcal{F}^a(A)$ ([1] 2.3), and the canonical surjection $\mathcal{F}(A) \to \mathcal{F}^a(A)$ is a homomorphism of $\mathcal{G}_K$-groups. Hence, the kernel $G^a(\overline{K}) = \mathrm{Ker}(\mathcal{F}(A) \to \mathcal{F}^a(A))$ defines a subgroup scheme G^a_η of G_η over η, and the schematic closure G^a of G^a_η in G is a closed subgroup scheme of G, locally free of finite type over S. We put $G^0 = G$. The exhaustive decreasing filtration $(G^a, a \in \mathbb{Q}_{\geq 0})$ defined above is called *the canonical filtration of* G ([1] 2.3.1). Lemma 2.3 gives immediately the following.

Lemma 2.6. *Let K'/K be an extension (not necessarily finite) of complete discrete valuation fields with ramification index $e_{K'/K}$, $\mathcal{O}_{K'}$ be the ring of integers of K', and $\overline{K'}$ be an algebraic closure of K' containing $\overline{K}$. Let G be an object of* Gr_S *and $G' = G \times_S \mathrm{Spec}(\mathcal{O}_{K'})$. Then we have a canonical isomorphism $G^a(\overline{K}) \simeq G'^{ae_{K'/K}}(\overline{K'})$ for all $a \in \mathbb{Q}_{>0}$.*

2.7. For an object G of Gr_S and $a \in \mathbb{Q}_{\geq 0}$, we denote $G^{a+} = \cup_{b>a}G^b$ and if $a > 0$, $G^{a-} = \cap_{0<b<a}G^b$, where b runs over rational numbers. The construction of the canonical filtration is functorial: a morphism $u : G \to H$ of Gr_S induces canonical homomorphisms $u^a : G^a \to H^a$, $u^{a+} : G^{a+} \to H^{a+}$ and $u^{a-} : G^{a-} \to H^{a-}$.

Proposition 2.8 ([1] Lemmes 2.3.2 and 2.3.5)**.** (i) *For any object G of* Gr_S*, G^{0+} is the neutral connected component of G.*

(ii) *Let $u : G \to H$ be a finite flat and surjective morphism in* Gr_S *and $a \in \mathbb{Q}_{>0}$. Then the homomorphism $u^a(\overline{K}) : G^a(\overline{K}) \to H^a(\overline{K})$ is surjective.*

2.9. Let A and B be two abelian schemes over S, $\phi : A \to B$ be an isogeny (*i.e.* a finite flat morphism of group schemes), and G be the kernel of ϕ. Let ν (*resp.* μ) be the generic point of the special fiber A_s (*resp.* B_s), and $\widehat{\mathcal{O}}_\nu$ (*resp.* $\widehat{\mathcal{O}}_\mu$) be the completion of the local ring of A at ν (*resp.* of B at μ). Let M and L be the fraction fields of $\widehat{\mathcal{O}}_\nu$ and $\widehat{\mathcal{O}}_\mu$ respectively. So we have the cartesian diagram

$$\begin{tikzcd} \operatorname{Spec} M \arrow[r] \arrow[d] & \operatorname{Spec} \widehat{\mathcal{O}}_\nu \arrow[r] \arrow[d] & A \arrow[d] \\ \operatorname{Spec} L \arrow[r] & \operatorname{Spec} \widehat{\mathcal{O}}_\mu \arrow[r] & B \end{tikzcd}$$

We fix a separable closure $\overline{L}$ of L containing $\overline{K}$, and an imbedding of M in $\overline{L}$. Since $\phi : A \to B$ is a G-torsor, M/L is a Galois extension, and we have a canonical isomorphism

$$G(\overline{K}) = \mathcal{F}_K(G) \xrightarrow{\sim} \mathcal{F}_L(\widehat{\mathcal{O}}_\nu) = \mathrm{Gal}(M/L). \tag{2.9.1}$$

Using the same arguments of ([1] 2.4.2), we prove the following

Proposition 2.10. *For all rational numbers $a \geq 0$, the isomorphism* (2.9.1) *induces an isomorphism $G^a(\overline{K}) \simeq \mathrm{Gal}(M/L)^a$.*

3. Review of the abelian scheme case following [1]

From this section on, we assume that the residue field k of $\mathcal{O}_K$ is perfect of characteristic $p > 0$.

3.1. Let X be a smooth and proper scheme over S, and $\overline{X} = X \times_S \overline{S}$. We consider the cartesian diagram

$$\begin{tikzcd} X_{\overline{s}} \arrow[r, "\overline{i}"] \arrow[d] & \overline{X} \arrow[d] & X_{\overline{\eta}} \arrow[l, "\overline{j}"'] \arrow[d] \\ \overline{s} = \operatorname{Spec} \overline{k} \arrow[r] & \overline{S} & \overline{\eta} = \operatorname{Spec} \overline{K} \arrow[l] \end{tikzcd}$$

and the sheaves of p-adic vanishing cycles on $X_{\overline{s}}$

$$\Psi_X^q = \overline{i}^* R^q \overline{j}_* (\mathbb{Z}/p\mathbb{Z}(q)), \tag{3.1.1}$$

where $q \geq 0$ is an integer and $\mathbb{Z}/p\mathbb{Z}(q)$ is the Tate twist of $\mathbb{Z}/p\mathbb{Z}$. It is clear that $\Psi_X^0 \simeq \mathbb{Z}/p\mathbb{Z}$. By the base change theorem for proper morphisms, we have a spectral sequence

$$E_2^{p,q}(X) = \mathrm{H}^p(X_{\overline{s}}, \Psi_X^q)(-q) \Longrightarrow \mathrm{H}^{p+q}(X_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z}), \tag{3.1.2}$$

which induces an exact sequence

$$0 \to \mathrm{H}^1(X_{\overline{s}}, \mathbb{Z}/p\mathbb{Z}) \to \mathrm{H}^1(X_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z}) \xrightarrow{u} \mathrm{H}^0(X_{\overline{s}}, \Psi_X^1)(-1) \to \mathrm{H}^2(X_{\overline{s}}, \mathbb{Z}/p\mathbb{Z}). \tag{3.1.3}$$

3.2. The Kummer's exact sequence $0 \to \mu_p \to \mathbb{G}_m \to \mathbb{G}_m \to 0$ on $X_{\overline{\eta}}$ induces the symbol map

$$h_{\overline{X}} : \overline{i}^* \overline{j}_* \mathcal{O}_{X_{\overline{\eta}}}^\times \to \Psi_X^1. \tag{3.2.1}$$

We put $\mathrm{U}^0 \Psi_X^1 = \Psi_X^1$, and for $a \in \mathbb{Q}_{>0}$,

$$\mathrm{U}^a \Psi_X^1 = h_{\overline{X}}(1 + \pi^a \overline{i}^* \mathcal{O}_{\overline{X}}), \tag{3.2.2}$$

where by abuse of notation π^a is an element in $\mathcal{O}_{\overline{K}}$ with $v(\pi^a) = a$. We have $\mathrm{U}^a \Psi_X^1 = 0$ if $a \geq \frac{ep}{p-1}$ ([1] Lemme 3.1.1).

Passing to the cohomology, we get a filtration on $\mathrm{H}^1(X_{\overline{\eta}},\mathbb{Z}/p\mathbb{Z})$ defined by:

$$\begin{aligned}&\mathrm{U}^0\mathrm{H}^1(X_{\overline{\eta}},\mathbb{Z}/p\mathbb{Z})=\mathrm{H}^1(X_{\overline{\eta}},\mathbb{Z}/p\mathbb{Z}),\\ &\mathrm{U}^a\mathrm{H}^1(X_{\overline{\eta}},\mathbb{Z}/p\mathbb{Z})=u^{-1}(\mathrm{H}^0(X_{\overline{s}},\mathrm{U}^a\Psi^1_X)(-1)),\quad \text{for } a\in\mathbb{Q}_{>0},\end{aligned}\tag{3.2.3}$$

called the *Bloch-Kato filtration*.

Theorem 3.3 ([1] Théorème 3.1.2)**.** *Let A be an abelian scheme over S, ${}_pA$ its kernel of multiplication by p, and $e'=\frac{ep}{p-1}$. Then under the canonical perfect pairing*

$$ {}_pA(\overline{K})\times\mathrm{H}^1(A_{\overline{\eta}},\mathbb{Z}/p\mathbb{Z})\to\mathbb{Z}/p\mathbb{Z},\tag{3.3.1}$$

we have for all $a\in\mathbb{Q}_{\geq 0}$,

$$ {}_pA^{a+}(\overline{K})^{\perp}=\begin{cases}\mathrm{U}^{e'-a}\mathrm{H}^1(A_{\overline{s}},\mathbb{Z}/p\mathbb{Z}) & \text{if } 0\leq a\leq e';\\ \mathrm{H}^1(A_{\overline{\eta}},\mathbb{Z}/p\mathbb{Z}) & \text{if } a>e'.\end{cases}$$

3.4. Let X be a scheme over S, $\overline{X}=X\times_S\overline{S}$. For all $a\in\mathbb{Q}_{>0}$, we put $\overline{S}_a=\mathrm{Spec}(\mathcal{O}_{\overline{K}}/\mathfrak{m}_a)$ and $\overline{X}_a=X\times_S\overline{S}_a$ (1.9). We denote by $\mathbf{D}((\overline{X}_1)_{\text{ét}})$ the derived category of abelian étale sheaves over $\overline{X}_1$. A morphism of schemes is called *syntomic*, if it is flat and of complete intersection.

Let X be a syntomic and quasi-projective S-scheme, r and n be integers with $r\geq 0$ and $n\geq 1$. In [13], Kato constructed a canonical object $\mathfrak{J}^{[r]}_{n,\overline{X}}$ in $\mathbf{D}((\overline{X}_1)_{\text{ét}})$, and if $0\leq r\leq p-1$ a morphism $\varphi_r:\mathfrak{J}^{[r]}_{n,\overline{X}}\to\mathfrak{J}^{[0]}_{n,\overline{X}}$, which can be roughly seen as "$1/p^r$ times of the Frobenius map". We refer to [13] and ([1] 4.1.6) for details of these constructions. Let $\mathcal{S}_n(r)_{\overline{X}}$ be the fiber cone of the morphism φ_r-1 for $0\leq r\leq p-1$; so we have a distinguished triangle in $\mathbf{D}((\overline{X}_1)_{\text{ét}})$

$$\mathcal{S}_n(r)_{\overline{X}}\to\mathfrak{J}^{[r]}_{n,\overline{X}}\xrightarrow{\varphi_r-1}\mathfrak{J}^{[0]}_{n,\overline{X}}\xrightarrow{+1}.\tag{3.4.1}$$

The complexes $\mathcal{S}_n(r)_{\overline{X}}$ $(0\leq r\leq p-1)$ are called the *syntomic complexes* of $\overline{X}$. For our purpose, we recall here some of their properties for $r=1$.

3.5. According to ([13] section I.3), for any integer $n\geq 1$, there exists a surjective symbol map

$$\mathcal{O}^{\times}_{\overline{X}_{n+1}}\to\mathcal{H}^1(\mathcal{S}_n(1)_{\overline{X}}).$$

For a geometric point $\overline{x}$ of $X_{\overline{s}}$, we put

$$\mathfrak{S}^1_{\overline{x}}=\left(\mathcal{O}_{\overline{X},\overline{x}}[\frac{1}{p}]\right)^{\times}=(\overline{i}^*\overline{j}_*\mathcal{O}^{\times}_{X_{\overline{\eta}}})_{\overline{x}}.$$

By ([13] I.4.2), the above symbol map at $\overline{x}$ factorizes through the canonical surjection $\mathcal{O}^{\times}_{\overline{X},\overline{x}}\to\mathfrak{S}^1_{\overline{x}}/p^n\mathfrak{S}^1_{\overline{x}}$.

Theorem 3.6 ([13] I.4.3)**.** *Assume that $p\geq 3$. Let X be a smooth and quasi-projective scheme over S. Then there is a canonical isomorphism $\mathcal{H}^1(\mathcal{S}_1(1)_{\overline{X}})\xrightarrow{\sim}\Psi^1_X$, which is compatible with the symbol maps $\mathfrak{S}^1_{\overline{x}}\to\mathcal{H}^1(\mathcal{S}_1(1)_{\overline{X}})_{\overline{x}}$ and $h_{\overline{X}}:\mathfrak{S}^1_{\overline{x}}\to\Psi^1_{X,\overline{x}}$ (3.2.1).*

3.7. Let X be a smooth and quasi-projective scheme over S. Let $\phi_{\overline{X}_1}$ and $\phi_{\overline{S}_1}$ be the absolute Frobenius morphisms of $\overline{X}_1$ and $\overline{S}_1$, and let $\overline{X}_1^{(p)}$ be the scheme defined by the cartesian diagram

$$\begin{tikzcd} \overline{X}_1^{(p)} \arrow[r, "w"] \arrow[d] & \overline{X}_1 \arrow[d] \\ \overline{S}_1 \arrow[r, "\phi_{\overline{S}_1}"] & \overline{S}_1. \end{tikzcd}$$

For all integers $q \geq 0$, we denote by F the composed morphism

$$\Omega^q_{\overline{X}_1/\overline{S}_1} \xrightarrow{w^*} \Omega^q_{\overline{X}_1^{(p)}/\overline{S}_1} \to \Omega^q_{\overline{X}_1/\overline{S}_1}/d(\Omega^{q-1}_{\overline{X}_1/\overline{S}_1}),$$

where the second morphism is induced by the Cartier isomorphism

$$C^{-1}_{\overline{X}_1/\overline{S}_1} : \Omega^q_{\overline{X}_1^{(p)}/\overline{S}_1} \xrightarrow{\sim} \mathcal{H}^q(\Omega^\bullet_{\overline{X}_1/\overline{S}_1}).$$

Let c be the class in $\mathcal{O}_{\overline{S}_1}$ of a p-th root of $(-p)$. We set

$$\mathcal{P} = \mathrm{Coker}\Big(\mathcal{O}_{\overline{X}_1} \xrightarrow{\mathrm{F}-c} \mathcal{O}_{\overline{X}_1}\Big), \tag{3.7.1}$$

$$\mathcal{Q} = \mathrm{Ker}\Big(\Omega^1_{\overline{X}_1/\overline{S}_1} \xrightarrow{\mathrm{F}-1} \Omega^1_{\overline{X}_1/\overline{S}_1}/d(\mathcal{O}_{\overline{X}_1})\Big).$$

Proposition 3.8 ([1] 4.1.8)**.** *The notations are those as above, and we assume moreover that $p \geq 3$. Let $\overline{x}$ be a geometric point in $X_{\overline{s}}$.*

(i) *There exist canonical isomorphisms*

$$\mathcal{P} \xrightarrow{\sim} \mathrm{Coker}\Big(\mathcal{H}^0(\mathfrak{I}^{[1]}_{1,\overline{X}}) \xrightarrow{\varphi_1 - 1} \mathcal{H}^0(\mathfrak{I}^{[0]}_{1,\overline{X}})\Big), \quad \mathcal{Q} \xrightarrow{\sim} \mathrm{Ker}\Big(\mathcal{H}^1(\mathfrak{I}^{[1]}_{1,\overline{X}}) \xrightarrow{\varphi_1 - 1} \mathcal{H}^1(\mathfrak{I}^{[0]}_{1,\overline{X}})\Big),$$

so the distinguished triangle (3.4.1) *gives rise to an exact sequence*

$$0 \to \mathcal{P} \xrightarrow{\alpha} \mathcal{H}^1(\mathcal{S}_1(1)_{\overline{X}}) \xrightarrow{\beta} \mathcal{Q} \to 0. \tag{3.8.1}$$

(ii) *Let $e(T) = \sum_{i=0}^{p-1} T^i/i! \in \mathbb{Z}_p[T]$. Then the morphism $\alpha_{\overline{x}}$ in* (3.8.1) *is induced by the map $\mathcal{O}_{\overline{X}_1,\overline{x}} \to \mathfrak{S}^1_{\overline{x}}/p\mathfrak{S}^1_{\overline{x}}$ given by*

$$a \mapsto e(-\tilde{a}(\zeta - 1)^{p-1}),$$

where $\tilde{a}$ is a lift of $a \in \mathcal{O}_{\overline{X}_1,\overline{x}}$ and $\zeta \in \overline{K}$ is a primitive p-th root of unity.

(iii) *The composed map*

$$\mathfrak{S}^1_{\overline{x}}/p\mathfrak{S}^1_{\overline{x}} \xrightarrow{\text{symbol}} \mathcal{H}^1(\mathcal{S}_1(1)_{\overline{X}})_{\overline{x}} \xrightarrow{\beta} \mathcal{Q}_{\overline{x}}$$

is the unique morphism sending $a \in \mathcal{O}^\times_{\overline{X},\overline{x}}$ to $a^{-1}da \in \mathcal{Q}_{\overline{x}}$.

Remark 3.9. Statement (ii) of Proposition 3.8 implies that, via the canonical isomorphism $\mathcal{H}^1(\mathcal{S}_1(1)_{\overline{X}}) \simeq \Psi^1_X$ (3.6), $\mathcal{P}$ can be identified with the submodule $\mathrm{U}^e\Psi^1_X$ of Ψ^1_X defined in (3.2.2).

Proposition 3.10 ([1] 4.1.9)**.** *Assume that $p \geq 3$. Let X be a smooth projective scheme over S, $t = (p-1)/p$.*

(i) *The morphism $\mathrm{F} - c : \mathcal{O}_{\overline{X}_1} \to \mathcal{O}_{\overline{X}_1}$ factorizes through the quotient morphism $\mathcal{O}_{\overline{X}_1} \to \mathcal{O}_{\overline{X}_t}$, and we have an exact sequence*

$$0 \to \mathbb{F}_p \to \mathcal{O}_{\overline{X}_t} \xrightarrow{\mathrm{F}-c} \mathcal{O}_{\overline{X}_1} \to \mathcal{P} \to 0. \tag{3.10.1}$$

(ii) *Let* $\delta_E : \mathrm{H}^0(\overline{X}_1, \mathcal{P}) \to \mathrm{H}^2(\overline{X}_1, \mathbb{F}_p)$ *be the cup-product with the class of (3.10.1) in* $\mathrm{Ext}^2(\mathcal{P}, \mathbb{F}_p)$, *and*

$$d_2^{0,1} : \mathrm{H}^0(\overline{X}_{\overline{s}}, \Psi^1_X)(-1) \to \mathrm{H}^2(\overline{X}_{\overline{s}}, \mathbb{F}_p)$$

be the connecting morphism in (3.1.3)*. Then the composed morphism*

$$\mathrm{H}^0(\overline{X}_1, \mathcal{P}) \to \mathrm{H}^0(\overline{X}_{\overline{s}}, \mathcal{H}^1(\mathcal{S}_1(1)_{\overline{X}})) \xrightarrow{\sim} \mathrm{H}^0(\overline{X}_{\overline{s}}, \Psi^1_X) \xrightarrow{d_2^{0,1}(1)} \mathrm{H}^2(\overline{X}_{\overline{s}}, \mathbb{F}_p)(1)$$

coincides with $\zeta\delta_E$*, where the middle isomorphism is given by Theorem 3.6, and* ζ *is a chosen* p*-th root of unity.*

(iii) *Assume moreover that* $\mathrm{H}^0(\overline{X}_r, \mathcal{O}_{\overline{X}_r}) = \mathcal{O}_{S_r}$ *for* $r = 1$ *and* t*. Then we have an exact sequence*

(3.10.2)
$$0 \to \mathrm{H}^1(X_{\overline{s}}, \mathbb{F}_p) \to \mathrm{Ker}\Big(\mathrm{H}^1(\overline{X}_1, \mathcal{O}_{\overline{X}_t}) \xrightarrow{\mathrm{F}-c} \mathrm{H}^1(\overline{X}_1, \mathcal{O}_{\overline{X}_1})\Big) \to \mathrm{H}^0(\overline{X}_1, \mathcal{P}) \xrightarrow{\delta_E} \mathrm{H}^2(X_{\overline{s}}, \mathbb{F}_p)$$

3.11. Let M be a free $\mathcal{O}_{\overline{S}_1}$-module of rank r and $\varphi : M \to M$ be a semi-linear endomorphism with respect to the absolute Frobenius of $\mathcal{O}_{\overline{S}_1}$. Following [1], we call M a *φ-$\mathcal{O}_{\overline{S}_1}$-module* of rank r. Then $\varphi(M)$ is an $\mathcal{O}_{\overline{S}_1}$-submodule of M, and there exist rational numbers $0 \leq a_1 \leq a_2 \leq \cdots \leq a_r \leq 1$, such that

$$M/\varphi(M) \simeq \oplus_{i=1}^r \mathcal{O}_{\overline{K}}/\mathfrak{m}_{a_i}.$$

We define the *Hodge height* of M to be $\sum_{i=1}^r a_i$. For any rational number $0 \leq t \leq 1$, we put $M_t = M \otimes_{\mathcal{O}_{\overline{S}_1}} \mathcal{O}_{\overline{S}_t}$.

Proposition 3.12 ([3] 9.1 and 9.7)**.** *Assume that* $p \geq 3$*. Let* λ *be an element in* $\mathcal{O}_{\overline{K}}$*, and* $r \geq 1$ *an integer. We assume* $v = v_p(\lambda) < \frac{1}{2}$ *and let* M *be a* φ-$\mathcal{O}_{\overline{S}_1}$*-module of rank* r *such that its Hodge height is strictly smaller than* v*.*

(i) *The morphism* $\varphi - \lambda : M \to M$ *factorizes through the canonical map* $M \to M_{1-v}$ *and the kernel of* $\varphi - \lambda : M_{1-v} \to M$ *is an* $\mathbb{F}_p$*-vector space of dimension* r*.*

(ii) *Let* N_0 *be the kernel of the morphism* $M_{1-v} \to M$ *induced by* $\varphi - \lambda$*, and* N *be the* $\mathcal{O}_{\overline{K}}$*-submodule of* M_{1-v} *generated by* N_0*. Then we have* $\dim_{\overline{k}}(N/\mathfrak{m}_{\overline{K}}N) = \dim_{\mathbb{F}_p} N_0 = r$*.*

3.13. We can now summarize the strategy of [1] as follows. Let A be a projective abelian scheme of dimension g over S. By Proposition 3.10(iii), we have

$$\begin{aligned}(3.13.1)\qquad \dim_{\mathbb{F}_p} \mathrm{H}^1(\overline{A}_1, \mathbb{F}_p) + \dim_{\mathbb{F}_p} \mathrm{Ker}\Big(\mathrm{H}^0(\overline{A}_1, \mathcal{P}) \xrightarrow{\delta_E} \mathrm{H}^2(\overline{A}_1, \mathbb{F}_p)\Big) \\ = \dim_{\mathbb{F}_p} \mathrm{Ker}\Big(\mathrm{H}^1(\overline{A}_1, \mathcal{O}_{\overline{A}_t}) \xrightarrow{\mathrm{F}-c} \mathrm{H}^1(\overline{A}_1, \mathcal{O}_{\overline{A}_1})\Big).\end{aligned}$$

By Remark 3.9 and Proposition 3.10(ii), the left hand side equals $\dim_{\mathbb{F}_p} \mathrm{U}^e\mathrm{H}^1(A_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z})$ (3.2.3). Taking account of Theorem 3.3, we get

$$(3.13.2)\qquad 2g - \dim_{\mathbb{F}_p}\big({}_pA^{j+}(\overline{K})\big) = \dim_{\mathbb{F}_p} \mathrm{Ker}\Big(\mathrm{H}^1(\overline{A}_1, \mathcal{O}_{\overline{X}_t}) \xrightarrow{\mathrm{F}-c} \mathrm{H}^1(\overline{A}_1, \mathcal{O}_{\overline{X}_1})\Big),$$

where $j = \frac{e}{p-1}$. Applying 3.12(i) to $M = \mathrm{H}^1(\overline{A}_1, \mathcal{O}_{\overline{X}_1})$ and $\lambda = c$, we obtain immediately the first statement of Theorem 1.4 for projective abelian schemes. In fact, Abbes and Mokrane proved a less optimal bound on the Hodge height ([1] 5.1.1).

4. Cohomological preliminaries

4.1. Let $f : X \to T$ be a proper, flat and finitely presented morphism of schemes. We work with the fppf-topology on T, and denote by $\mathrm{Pic}_{X/T}$ the relative Picard functor $R^1_{\mathrm{fppf}} f_*(\mathbb{G}_m)$.

If T is the spectrum of a field, $\mathrm{Pic}_{X/T}$ is representable by a group scheme locally of finite type over k. We denote by $\mathrm{Pic}^0_{X/T}$ the neutral component, and put $\mathrm{Pic}^\tau_{X/T} = \bigcup_{n\geq 1} n^{-1}\,\mathrm{Pic}^0_{X/T}$, where $n : \mathrm{Pic}_{X/T} \to \mathrm{Pic}_{X/T}$ is the multiplication by n. Then $\mathrm{Pic}^0_{X/T}$ and $\mathrm{Pic}^\tau_{X/T}$ are open sub-group schemes of $\mathrm{Pic}_{X/T}$.

For a general base, $\mathrm{Pic}_{X/T}$ is representable by an algebraic space over T ([4] thm. 7.3). We denote by $\mathrm{Pic}^0_{X/T}$ (*resp.* $\mathrm{Pic}^\tau_{X/T}$) the subfunctor of $\mathrm{Pic}_{X/T}$ which consists of all elements whose restriction to all fibres X_t, $t \in T$, belong to $\mathrm{Pic}^0_{X_t/t}$ (*resp.* $\mathrm{Pic}^\tau_{X_t/t}$). By (SGA 6 XIII, thm 4.7), the canonical inclusion $\mathrm{Pic}^\tau_{X/T} \to \mathrm{Pic}_{X/T}$ is relatively representable by an open immersion.

4.2. Let $f : A \to T$ be an abelian scheme. If T is the spectrum of a field, the Néron-Séveri group $\mathrm{Pic}_{A/T} / \mathrm{Pic}^0_{A/T}$ is torsion free, *i.e.* we have $\mathrm{Pic}^0_{A/T} = \mathrm{Pic}^\tau_{A/T}$. This coincidence remains true for a general base T by the definitions of $\mathrm{Pic}^0_{A/T}$ and $\mathrm{Pic}^\tau_{A/T}$. Moreover, $\mathrm{Pic}^\tau_{A/T}$ is formally smooth (cf. [18] Prop. 6.7), and $\mathrm{Pic}^\tau_{A/T}$ is actually open and closed in $\mathrm{Pic}_{A/T}$, and is representable by a proper and smooth algebraic space over T, *i.e.* an abelian algebraic space over T. By a theorem of Raynaud ([10] Ch. 1, thm. 1.9), every abelian algebraic space over T is automatically an abelian scheme over T. So $\mathrm{Pic}^0_{A/T} = \mathrm{Pic}^\tau_{A/T}$ is an abelian scheme, called the *dual abelian scheme of* A, and denoted by $A^\vee$.

Let H be a commutative group scheme locally free of finite type over T. Recall the following isomorphism due to Raynaud ([19] 6.2.1):

$$R^1_{\mathrm{fppf}} f_*(H_A) \xrightarrow{\sim} \mathcal{H}om(H^\vee, \mathrm{Pic}_{A/T}), \tag{4.2.1}$$

where $H_A = H \times_T A$, $H^\vee$ is the Cartier dual of H, and $\mathcal{H}om$ is taken for the fppf-topology on T.

Proposition 4.3. *Let A be an abelian scheme over a scheme T, and H a commutative group scheme locally free of finite type over T. Then we have canonical isomorphisms*

$$\mathcal{E}xt^1(A, H) \xrightarrow{\sim} \mathcal{H}om(H^\vee, A^\vee), \tag{4.3.1}$$

$$\mathrm{Ext}^1(A, H) \xrightarrow{\sim} \mathrm{H}^0_{\mathrm{fppf}}(T, \mathcal{E}xt^1(A, H)) \xrightarrow{\sim} \mathrm{Hom}(H^\vee, A^\vee). \tag{4.3.2}$$

Proof. For any fppf-sheaf E on T, we have

$$\mathcal{H}om(H^\vee, \mathcal{H}om(E, \mathbb{G}_m)) \simeq \mathcal{H}om(H^\vee \otimes_{\mathbb{Z}} E, \mathbb{G}_m) \simeq \mathcal{H}om(E, H).$$

Deriving this isomorphism of functors in E and putting $E = A$, we obtain a spectral sequence

$$E_2^{p,q} = \mathcal{E}xt^p(H^\vee, \mathcal{E}xt^q(A, \mathbb{G}_m)) \Longrightarrow \mathcal{E}xt^{p+q}(A, H).$$

Since $\mathcal{H}om(A, \mathbb{G}_m) = 0$, the exact sequence

$$0 \to E_2^{1,0} \to \mathcal{E}xt^1(A, H) \to E_2^{0,1} \to E_2^{2,0}$$

induces an isomorphism

$$\mathcal{E}xt^1(A, H) \simeq \mathcal{H}om(H^\vee, \mathcal{E}xt^1(A, \mathbb{G}_m)).$$

Then (4.3.1) follows from the canonical identification $\mathcal{E}xt^1(A, \mathbb{G}_m) \simeq A^\vee$ ([8] 2.4). For (4.3.2), the spectral sequence

$$E_2^{p,q} = \mathrm{H}^p_{\mathrm{fppf}}(T, \mathcal{E}xt^q(A, H)) \Longrightarrow \mathrm{Ext}^{p+q}(A, H)$$

induces a long exact sequence

$$0 \to \mathrm{H}^1_{\mathrm{fppf}}(T, \mathcal{H}om(A,H)) \to \mathrm{Ext}^1(A,H) \xrightarrow{(1)} \mathrm{H}^0_{\mathrm{fppf}}(T, \mathcal{E}xt^1(A,H)) \to \mathrm{H}^2_{\mathrm{fppf}}(T, \mathcal{H}om(A,H)).$$

Since $\mathcal{H}om(A,H) = 0$, the arrow (1) is an isomorphism, and (4.3.2) follows by applying the functor $\mathrm{H}^0_{\mathrm{fppf}}(T, \_)$ to (4.3.1). □

4.4. The assumptions are those of (4.3). We define a canonical morphism

$$\mathrm{Ext}^1(A,H) \to \mathrm{H}^1_{\mathrm{fppf}}(A,H) \tag{4.4.1}$$

as follows. Let a be an element in $\mathrm{Ext}^1(A,H)$ represented by the extension $0 \to H \to E \to A \to 0$. Then the fppf-sheaf E is representable by a scheme over T, and is naturally a H-torsor over A. The image of a by the homomorphism (4.4.1) is defined to be the class of the torsor E. Since this construction is functorial in T, by passing to sheaves, we obtain a canonical morphism

$$\mathcal{E}xt^1(A,H) \to R^1_{\mathrm{fppf}} f_*(H_A). \tag{4.4.2}$$

Via the isomorphisms (4.2.1) and (4.3.1), we check that (4.4.2) is induced by the canonical map $A^\vee = \mathrm{Pic}^0_{A/T} \to \mathrm{Pic}_{A/T}$.

Since H is faithfully flat and finite over T, the inverse image of the fppf-sheaf H by f is representable by H_A, *i.e.* we have $f^*(H) = H_A$. Therefore, we deduce an adjunction morphism

$$H \to R^0_{\mathrm{fppf}} f_*(H_A). \tag{4.4.3}$$

Proposition 4.5. *Let $f : A \to T$ be an abelian scheme, and H be a commutative group scheme locally free of finite type over T. Then the canonical maps* (4.4.2) *and* (4.4.3) *are isomorphisms.*

Proof. First, we prove that (4.4.2) is an isomorphism. By (4.2.1) and (4.3.1), we have to verify that the canonical morphism

$$\mathcal{H}om(H^\vee, A^\vee) \to \mathcal{H}om(H^\vee, \mathrm{Pic}_{A/T})$$

is an isomorphism. Let $g : H^\vee \to \mathrm{Pic}_{A/T}$ be a homomorphism over T. For every $t \in T$, the induced morphism $g_t : H^\vee_t \to \mathrm{Pic}_{A_t/t}$ falls actually in $\mathrm{Pic}^\tau_{A_t/t}$, because $H^\vee$ is a finite group scheme. Hence, by the definition of $\mathrm{Pic}^\tau_{A/T}$, the homomorphism g factorizes through the canonical inclusion $A^\vee = \mathrm{Pic}^\tau_{A/T} \to \mathrm{Pic}_{A/T}$; so the canonical morphism $\mathrm{Hom}(H^\vee, A^\vee) \to \mathrm{Hom}(H^\vee, \mathrm{Pic}_{A/T})$ is an isomorphsim.

Secondly, we prove that (4.4.3) is an isomorphism. For T-schemes U and G, we denote $G_U = G \times_T U$. We must verify that for any T-scheme U, the adjunction morphism

$$\varphi(U) : H(U) \to R^0_{\mathrm{fppf}} f_*(H_A)(U) = H(A_U) \tag{4.5.1}$$

is an isomorphism. We note that $H(U) = H_U(U)$ and $H(A_U) = H_U(A_U)$; therefore, up to taking base changes, it suffices to prove that $\varphi(T)$ (4.5.1) is an isomorphism. We remark that f is surjective, hence $\varphi(T)$ is injective. To prove the surjectivity of $\varphi(T)$, we take an element $h \in H(A)$, *i.e.* a morphism of T-schemes $h : A \to H$; by rigidity lemma for abelian schemes (cf. [18] Prop. 6.1), there exists a section $s : T \to H$ of the structure morphism $H \to T$ such that $s \circ f = h$. Hence we have $\varphi(T)(s) = h$, and $\varphi(T)$ is an isomorphism. □

Corollary 4.6. *Let T be the spectrum of a stirctly henselian local ring, $f : A \to T$ an abelian scheme, and H a finite étale group scheme over T. Then we have canonical isomorphisms*

$$\mathrm{H}^1_{\text{ét}}(A,H) \simeq \mathrm{H}^1_{\mathrm{fppf}}(A,H) \simeq \mathrm{Ext}^1(A,H).$$

Proof. The first isomorphism follows from the étaleness of H ([11], 11.7). For the second one, the "local-global" spectral sequence induces a long exact sequence

$$0 \to \mathrm{H}^1_{\mathrm{fppf}}(T, R^0_{\mathrm{fppf}} f_*(H_A)) \to \mathrm{H}^1_{\mathrm{fppf}}(A, H) \to \mathrm{H}^0_{\mathrm{fppf}}(T, R^1_{\mathrm{fppf}} f_*(H_A)) \to \mathrm{H}^2_{\mathrm{fppf}}(T, R^0_{\mathrm{fppf}} f_*(H_A)).$$

By Prop. 4.5, we have $R^0_{\mathrm{fppf}} f_*(H_A) = H$. Since T is strictly henselian and H étale, we have $\mathrm{H}^q_{\mathrm{fppf}}(T, H) = \mathrm{H}^q_{\text{ét}}(T, H) = 0$ for all integers $q \geq 1$. Therefore, we obtain $\mathrm{H}^1_{\mathrm{fppf}}(A, H) \xrightarrow{\sim} \mathrm{H}^0_{\mathrm{fppf}}(T, R^1_{\mathrm{fppf}} f_*(H_A))$, and the corollary follows from 4.5 and (4.3.2). □

4.7. Let T be a scheme, and G be a commutative group scheme locally free of finite type over T. We denote by $\mathbb{G}_a$ the additive group scheme, and by $\mathrm{Lie}(G^\vee)$ the Lie algebra of $G^\vee$. By Grothendieck's duality formula ([17] II §14), we have a canonical isomorphism

$$\mathrm{Lie}(G^\vee) \simeq \mathcal{H}om_T(G, \mathbb{G}_a), \tag{4.7.1}$$

where we have regarded G and $\mathbb{G}_a$ as abelian fppf-sheaves on T. If T is of characteristic p and G is a truncated Barsotti-Tate group over T, then $\mathrm{Lie}(G^\vee)$ is a locally free of finite type $\mathcal{O}_T$-module ([12] 2.2.1(c)).

Similarly, for an abelian scheme $f : A \to T$, we have a canonical isomorphism ([5] 2.5.8)

$$\mathrm{Lie}(A^\vee) \simeq \mathcal{E}xt^1_T(A, \mathbb{G}_a) \simeq R^1 f_*(\mathbb{G}_a). \tag{4.7.2}$$

In the sequel, we will frequently use the identifications (4.7.1) and (4.7.2) without any indications.

The following Lemma is indicated by W. Messing.

Lemma 4.8. *Let L be an algebraically closed field of characteristic $p > 0$, R be an L-algebra integral over L, and M be a module of finite presentation over R, equipped with an endomorphism φ semi-linear with respect to the Frobenius of R. Then the map $\varphi - 1 : M \to M$ is surjective.*

Proof. First, we reduce the lemma to the case $R = L$. Consider R as a filtrant inductive limit of finite L-algebras $(R_i)_{i\in I}$. Since M is of finite presentation, there exists an $i \in I$, and an R_i-module M_i of finite presentation endowed with a Frobenius semi-linear endomorphism φ_i, such that $M = M_i \otimes_{R_i} R$ and $\varphi = \varphi_i \otimes \sigma$, where σ is the Frobenius on R. For $j \geq i$, we put $M_j = M_i \otimes_{R_i} R_j$ and $\varphi_j = \varphi_i \otimes_{R_i} \sigma_j$, where σ_j is the Frobenius of R_j. In order to prove $\varphi - 1$ is surjective on M, it is sufficient to prove the surjectivity of $\varphi_j - 1$ on each M_j for $j \geq i$. Therefore, we may assume that R is a finite dimensional L-algebra, and M is thus a finite dimensional vector space over L.

We put $M_1 = \bigcup_{n\geq 1} \mathrm{Ker}(\varphi^n)$ and $M_2 = \bigcap_{n\geq 1} \mathrm{Im}(\varphi^n)$. Then we have a decomposition $M = M_1 \oplus M_2$ as φ-modules, such that φ is nilpotent on M_1 and bijective on M_2 (Bourbaki, Algèbre VIII §2 n° 2 Lemme 2). Therefore, it is sufficient to prove the surjectivity of $\varphi - 1$ in the following two cases:

(i) φ is nilpotent. In this case, the endomorphism $1 - \varphi$ admits an inverse $1 + \sum_{n\geq 1} \varphi^n$. Hence it is surjective.

(ii) φ is invertible. We choose a basis of M over L, and let $U = (a_{i,j})_{1\leq i,j\leq n}$ be the matrix of φ in this basis. The problem reduces to prove that the equation system $\sum_{j=1}^n a_{i,j} x_j^p - x_i = b_i$ $(1 \leq i \leq n)$ in $X = (x_1, \cdots, x_n)$ has solutions for all $b = (b_1, \cdots, b_n) \in L^n$. Since U is invertible, let $V = (c_{i,j})_{1\leq i,j\leq n}$ be its inverse. Then the equation system $\sum_{j=1}^n a_{i,j} x_j^p - x_i = b_i$ is equivalent to $x_i^p - \sum_{j=1}^n c_{i,j} x_j = b'_i$ for $1 \leq i \leq n$ with $b' = \sum_j c_{i,j} b_j$. But these n equations define a finite étale cover of $\mathrm{Spec}\, L$ of degree p^n. Hence they admit solutions in L, since L is separably closed. This completes the proof. □

Corollary 4.9. *Let H be a Barsotti-Tate group or an abelian scheme over $\overline{S}_1$ (1.9). Then $\mathrm{Ext}^2(H, \mathbb{F}_p) = 0$ for the* fppf *topology on $\overline{S}_1$.*

Proof. Let K_0 be the fraction field of the ring of Witt vectors with coefficients in k; so K is a finite extension of degree e of K_0. Let $\mathcal{O}_{K_0}^{ur}$ be the ring of integers of the maximal unramified extension of K_0 in $\overline{K}$. Then $\mathcal{O}_{\overline{S}_1} = \mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}}$ is integral over the algebraically closed field $\overline{k} = \mathcal{O}_{K_0}^{ur}/p\mathcal{O}_{K_0}^{ur}$. As $\mathrm{Ext}^2(H, \mathbb{G}_a) = 0$ ([5] Proposition 3.3.2), the Artin-Schreier's exact sequence $0 \to \mathbb{F}_p \to \mathbb{G}_a \xrightarrow{\mathrm{F}-1} \mathbb{G}_a \to 0$ induces an exact sequence

$$\mathrm{Ext}^1(H, \mathbb{G}_a) \xrightarrow{\varphi-1} \mathrm{Ext}^1(H, \mathbb{G}_a) \to \mathrm{Ext}^2(H, \mathbb{F}_p) \to 0.$$

Since $\mathrm{Ext}^1(H, \mathbb{G}_a)$ is a free $\mathcal{O}_{\overline{S}_1}$-module ([5] 3.3.2.1), the corollary follows immediately from Lemma 4.8. □

5. The Bloch-Kato filtration for finite flat group schemes killed by p

5.1. Recall the following theorem of Raynaud ([5] 3.1.1): *Let T be a scheme, G be a commutative group scheme locally free of finite type over T. Then locally for the Zariski topology, there exists a projective abelian scheme A over T, such that G can be identified to a closed subgroup of A.*

In particular, if G is a commutative finite and flat group scheme over $S = \mathrm{Spec}(\mathcal{O}_K)$, we have an exact sequence of abelian fppf-sheaves over S

$$0 \to G \to A \to B \to 0, \tag{5.1.1}$$

where A and B are projective abelian schemes over S. In the sequel, such an exact sequence is called a *resolution of G by abelian schemes*.

5.2. Let $f : X \to Y$ be a morphism of proper and smooth S-schemes. For any integer $q \geq 0$, we have a base change morphism $f_{\overline{s}}^*(\Psi_Y^q) \to \Psi_X^q$ of p-adic vanishing cycles (3.1.1) (SGA 7 XIII 1.3.7.1). For $q = 1$, this morphism respects the Bloch-Kato filtrations (3.2.2), that is, it sends $f_{\overline{s}}^*(\mathrm{U}^a\Psi_Y^1)$ to $\mathrm{U}^a\Psi_X^1$ for all $a \in \mathbb{Q}_{\geq 0}$.

Passing to cohomology, we get a functorial map $\mathrm{H}^p(Y_{\overline{s}}, \Psi_Y^q)(-q) \to \mathrm{H}^p(X_{\overline{s}}, \Psi_X^q)(-q)$ for each pair of integers $p, q \geq 0$. These morphisms piece together to give a morphism of spectral sequences (3.1.2) $E_2^{(p,q)}(Y) \to E_2^{(p,q)}(X)$, which converges to the map $\mathrm{H}^{p+q}(Y_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z}) \to \mathrm{H}^{p+q}(X_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z})$ induced by $f_{\overline{\eta}}^*$. Therefore, we have the following commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{H}^1(Y_{\overline{s}}, \mathbb{Z}/p\mathbb{Z}) \arrow[r] \arrow[d, "\alpha_1"] & \mathrm{H}^1(Y_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z}) \arrow[r] \arrow[d, "\alpha_2"] & \mathrm{H}^0(Y_{\overline{s}}, \Psi_Y^1)(-1) \arrow[r, "d_2^{1,0}"] \arrow[d, "\alpha_3"] & \mathrm{H}^2(Y_{\overline{s}}, \mathbb{Z}/p\mathbb{Z}) \arrow[d, "\alpha_4"] \\
0 \arrow[r] & \mathrm{H}^1(X_{\overline{s}}, \mathbb{Z}/p\mathbb{Z}) \arrow[r] & \mathrm{H}^1(X_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z}) \arrow[r] & \mathrm{H}^0(X_{\overline{s}}, \Psi_X^1)(-1) \arrow[r, "d_2^{1,0}"] & \mathrm{H}^2(X_{\overline{s}}, \mathbb{Z}/p\mathbb{Z}).
\end{tikzcd} \tag{5.2.1}$$

It is clear that the Bloch-Kato filtration on $\mathrm{H}^1(X_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z})$ (3.2.3) is functorial in X. More precisely, the following diagram is commutative:

$$\begin{tikzcd}
\mathrm{U}^a\mathrm{H}^1(Y_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z}) \arrow[r, hook] \arrow[d] & \mathrm{H}^1(Y_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z}) \arrow[d, "\alpha_2"] \\
\mathrm{U}^a\mathrm{H}^1(X_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z}) \arrow[r, hook] & \mathrm{H}^1(X_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z})
\end{tikzcd} \tag{5.2.2}$$

5.3. Let G be a commutative finite and flat group scheme over S killed by p, and $0 \to G \to A \to B \to 0$ a resolution of G by abelian schemes (5.1.1). We apply the construction (5.2.1) to the morphism $A \to B$. Using Corollary 4.6, we obtain immediately that

$$\begin{aligned}
\operatorname{Ker} \alpha_2 &= \operatorname{Ker}\Big(\operatorname{Ext}^1(B_{\overline{\eta}}, \mathbb{F}_p) \to \operatorname{Ext}^1(A_{\overline{\eta}}, \mathbb{F}_p)\Big) \\
&= \operatorname{Hom}(G_{\overline{\eta}}, \mathbb{F}_p) = G^\vee(\overline{K})(-1), \\
\operatorname{Ker} \alpha_1 &= \operatorname{Ker}\Big(\operatorname{Ext}^1(B_{\overline{s}}, \mathbb{F}_p) \to \operatorname{Ext}^1(A_{\overline{s}}, \mathbb{F}_p)\Big) \\
&= \operatorname{Hom}(G_{\overline{s}}, \mathbb{F}_p) = (G_{\text{ét}})^\vee(\overline{K})(-1),
\end{aligned}$$

where $G_{\text{ét}} = G/G^{0+}$ is the étale part of G (cf. 2.8). Setting $N = \operatorname{Ker} \alpha_3$, we can complete (5.2.1) as follows:

(5.3.1)

$$\begin{tikzcd}
0 \arrow[r] & (G_{\text{ét}})^\vee(\overline{K})(-1) \arrow[r] \arrow[d, hook, "\gamma_1"] & G^\vee(\overline{K})(-1) \arrow[r, "u"] \arrow[d, hook, "\gamma_2"] & N \arrow[r, dashed] \arrow[d, hook, "\gamma_3"] & 0 \arrow[d, dashed] \\
0 \arrow[r] & \mathrm{H}^1(B_{\overline{s}}, \mathbb{Z}/p\mathbb{Z}) \arrow[r] \arrow[d, "\alpha_1"] & \mathrm{H}^1(B_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z}) \arrow[r] \arrow[d, "\alpha_2"] & \mathrm{H}^0(B_{\overline{s}}, \Psi^1_B)(-1) \arrow[r, "d_2^{1,0}(B)"] \arrow[d, "\alpha_3"] & \mathrm{H}^2(B_{\overline{s}}, \mathbb{Z}/p\mathbb{Z}) \arrow[d, "\alpha_4"] \\
0 \arrow[r] & \mathrm{H}^1(A_{\overline{s}}, \mathbb{Z}/p\mathbb{Z}) \arrow[r] & \mathrm{H}^1(A_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z}) \arrow[r] & \mathrm{H}^0(A_{\overline{s}}, \Psi^1_A)(-1) \arrow[r, "d_2^{1,0}(A)"] & \mathrm{H}^2(A_{\overline{s}}, \mathbb{Z}/p\mathbb{Z}).
\end{tikzcd}$$

We will show later that the morphism u is surjective.

Definition 5.4. The assumptions are those of 5.3. We call the *Bloch-Kato filtration* on $G^\vee(\overline{K})$, and denote by $(\mathrm{U}^a G^\vee(\overline{K}), a \in \mathbb{Q}_{\geq 0})$, the decreasing and exhaustive filtration defined by $\mathrm{U}^0 G^\vee(\overline{K}) = G^\vee(\overline{K})$, and for $a \in \mathbb{Q}_{>0}$,

$$\mathrm{U}^a G^\vee(\overline{K}) = \gamma_2^{-1}(\mathrm{U}^a \mathrm{H}^1(B_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z}))(1). \tag{5.4.1}$$

Proposition 5.5. *Let $e' = \frac{ep}{p-1}$, G be a commutative finite and flat group scheme over S killed by p, and $0 \to G \to A \to B \to 0$ be a resolution of G by abelian schemes* (5.1.1).

(i) *For all $a \in \mathbb{Q}_{\geq 0}$, we have*

$$\begin{aligned}
\mathrm{U}^a G^\vee(\overline{K}) &\simeq \operatorname{Ker}\Big(\mathrm{U}^a \mathrm{H}^1(B_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z})(1) \xrightarrow{\alpha_2(1)} \mathrm{U}^a \mathrm{H}^1(A_{\overline{\eta}}, \mathbb{Z}/p\mathbb{Z})(1)\Big) \\
&\simeq u^{-1}\Big(N(1) \cap \mathrm{H}^0(B_{\overline{s}}, \mathrm{U}^a \Psi^1(B))\Big),
\end{aligned} \tag{5.5.1}$$

where $N(1)$ is identified to a subgroup of $\mathrm{H}^0(B_{\overline{s}}, \Psi^1(B))$ by $\gamma_3(1)$ in (5.3.1).

(ii) *The morphism $u : G^\vee(\overline{K})(-1) \to N$ in* (5.3.1) *is surjective. In particular, N is contained in the kernel of the morphism $d_2^{1,0}(B)$ in* (5.3.1).

(iii) *Under the canonical perfect pairing*

$$G(\overline{K}) \times G^\vee(\overline{K}) \to \mu_p(\overline{K}), \tag{5.5.2}$$

we have, for all $a \in \mathbb{Q}_{\geq 0}$,

$$G^{a+}(\overline{K})^\perp = \begin{cases} \mathrm{U}^{e'-a} G^\vee(\overline{K}) & \text{if } 0 \leq a \leq e'; \\ G^\vee(\overline{K}) & \text{if } a > e'. \end{cases}$$

In particular, the filtration $(\mathrm{U}^a G^\vee(\overline{K}), a\in\mathbb{Q}_{\geq 0})$ *does not depend on the resolution of* G *by abelian schemes.*

Proof. Statement (i) is obvious from definition 5.4 and diagrams (5.2.2) and (5.3.1).

For (ii) and (iii), thanks to Lemma 2.6, we need only to prove the proposition after a base change $\mathcal{O}_K\to\mathcal{O}_{K'}$, where K'/K is a finite extension. Therefore, up to such a base change, we may add the following assumptions.

(1) We may assume that k is algebraically closed, K contains a primitive p-th root of unity, and $G(\overline{K})=G(K)$.

(2) For $X=A$ or B, we consider the cartesian diagram

$$\begin{tikzcd} X_s \arrow[r, "i"] \arrow[d] & X \arrow[d] & X_\eta \arrow[l, "j"'] \arrow[d] \\ s=\overline{s} \arrow[r] & S & \eta \arrow[l] \end{tikzcd}$$

and the étale sheaf $\Psi^1_{X,K}=i^*R^1j_*(\mathbb{Z}/p\mathbb{Z})$ over X_s. By an argument as in the proof of ([1] 3.1.1), we may assume that $\mathrm{H}^0(X_s,\Psi^1_X)=\mathrm{H}^0(X_s,\Psi^1_{X,K})$.

Since $\mathrm{U}^a\Psi^1_X=0$ for $a\geq e'$ ([1] Lemme 3.1.1), we have $\mathrm{U}^{e'}G^\vee(\overline{K})=\mathrm{Ker}(u)(1)=(G_{\text{ét}})^\vee(\overline{K})$. Statement (iii) for $a=0$ follows immediately from Proposition 2.8(i). The pairing (5.5.2) induces a perfect pairing

$$G^{0+}(\overline{K})\times \mathrm{Im}(u)(1)\longrightarrow \mu_p(\overline{K}). \tag{5.5.3}$$

In particular, we have $\dim_{\mathbb{F}_p}\big(\mathrm{Im}(u)(1)\big)=\dim_{\mathbb{F}_p}\big(G^{0+}(\overline{K})\big)$.

Let μ (*resp.* ν) be the generic point of $B_s=B_{\overline{s}}$ (*resp.* of $A_s=A_{\overline{s}}$), and $\overline{\nu}$ be a geometric point over ν. Then $\overline{\nu}$ induces by the morphism $\nu\to\mu$ a geometric point over μ, denoted by $\overline{\mu}$. Let $\mathcal{O}_\mu$ (*resp.* $\mathcal{O}_\nu$) be the local ring of B at μ (*resp.* of A at ν), $\mathcal{O}_{\overline{\mu}}$ (*resp.* $\mathcal{O}_{\overline{\nu}}$) be the henselization of $\mathcal{O}_\mu$ at $\overline{\mu}$ (*resp.* of $\mathcal{O}_\nu$ at $\overline{\nu}$). We denote by $\widehat{\mathcal{O}}_\mu$ and $\widehat{\mathcal{O}}_\nu$ the completions of $\mathcal{O}_\mu$ and $\mathcal{O}_\nu$, and by $(\widehat{\mathcal{O}}_\mu)^{\mathrm{h}}_{\overline{\mu}}$ (*resp.* by $(\widehat{\mathcal{O}}_\nu)^{\mathrm{h}}_{\overline{\nu}}$) the henselization of $\widehat{\mathcal{O}}_\mu$ (*resp.* of $\widehat{\mathcal{O}}_\nu$) at $\overline{\mu}$ (*resp.* at $\overline{\nu}$). Let L_0 (*resp.* M_0) be the fraction field of $\mathcal{O}_\mu$ (*resp.* of $\mathcal{O}_\nu$), L_0^{ur} (*resp.* M_0^{ur}) be the fraction field of $\mathcal{O}_{\overline{\mu}}$ (*resp.* of $\mathcal{O}_{\overline{\nu}}$). We denote by L (*resp.* by M) the fraction field of $\widehat{\mathcal{O}}_\mu$ (*resp.* of $\widehat{\mathcal{O}}_\nu$), and by L^{ur} (*resp.* by M^{ur}) the fraction field of $(\widehat{\mathcal{O}}_\mu)^{\mathrm{h}}_{\overline{\mu}}$ (*resp.* of $(\widehat{\mathcal{O}}_\nu)^{\mathrm{h}}_{\overline{\nu}}$). We notice that π is a uniformizing element in $\widehat{\mathcal{O}}_\mu$ and in $(\widehat{\mathcal{O}}_\mu)^{\mathrm{h}}_{\overline{\mu}}$.

$$\begin{tikzcd} \mathcal{O}_{\overline{\mu}} \arrow[r] & L_0^{ur} \arrow[r] & L^{ur} & (\widehat{\mathcal{O}}_\mu)^{\mathrm{h}}_{\overline{\mu}} \arrow[l] \\ \mathcal{O}_\mu \arrow[r] \arrow[u] & L_0 \arrow[r] \arrow[u] & L \arrow[u] & \widehat{\mathcal{O}}_\mu \arrow[l] \arrow[u] \end{tikzcd}$$

Since $G=\mathrm{Ker}(A\to B)$, we have an identification $\mathrm{Gal}(M/L)\simeq G(K)=G(\overline{K})$. We fix a separable closure $\overline{L}$ of L, and an imbedding of M in $\overline{L}$, which induces a surjection $\varphi:\mathrm{Gal}(\overline{L}/L)\to\mathrm{Gal}(M/L)$. By 2.10, we have $\varphi(\mathrm{Gal}(\overline{L}/L)^a)=\mathrm{Gal}(M/L)^a=G^a(\overline{K})$, for all $a\in\mathbb{Q}_{>0}$. In particular, we have

$$\varphi(\mathrm{Gal}(\overline{L}/L^{ur}))=\mathrm{Gal}(M/M\cap L^{ur})=\mathrm{Gal}(M^{ur}/L^{ur})=G^{0+}(\overline{K}). \tag{5.5.4}$$

Since L^{ur}/L is unramified, we have, for all $a\in\mathbb{Q}_{>0}$,

$$\mathrm{Gal}(M^{ur}/L^{ur})^a=\mathrm{Gal}(M/L)^a=G^a. \tag{5.5.5}$$

Let ρ_B be the composition of the canonical morphisms

$$\mathrm{H}^0(B_s,\Psi^1_B)=\mathrm{H}^0(B_s,\Psi^1_{B,K})\to(\Psi^1_{B,K})_{\overline{\mu}}=\mathrm{H}^1(\mathrm{Spec}\,L_0^{ur},\mu_p)\to\mathrm{H}^1(\mathrm{Spec}\,L^{ur},\mu_p),$$

and we define ρ_A similarly. By functoriality and (5.5.4), we have a commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & N(1) \arrow[r] \arrow[d, hook] & \mathrm{H}^0(B_s,\Psi^1_B) \arrow[r] \arrow[d, hook, "\rho_B"] & \mathrm{H}^0(A_s,\Psi^1_A) \arrow[d, hook, "\rho_A"] \\ 0 \arrow[r] & \mathrm{H}^1(G^{0+}(\overline{K}),\mu_p) \arrow[r, "inf"] & \mathrm{H}^1(\mathrm{Spec}\,L^{ur},\mu_p) \arrow[r, "res"] & \mathrm{H}^1(\mathrm{Spec}\,M^{ur},\mu_p), \end{tikzcd} \tag{5.5.6}$$

where the lower horizontal row is the "inflation-restriction" exact sequence in Galois cohomology. By ([6] Prop. 6.1), ρ_B and ρ_A are injective. Hence $\mathrm{Im}(u)(1)\subset N(1)$ is identified with a subgroup of $\mathrm{H}^1(G^{0+}(\overline{K}),\mu_p)$. By assumption (1), we have $\mathrm{H}^1(G^{0+}(\overline{K}),\mu_p)=\mathrm{Hom}(G^{0+}(\overline{K}),\mu_p(\overline{K}))$, which has the same dimension over $\mathbb{F}_p$ as $G^{0+}(\overline{K})$. Hence by the remark below (5.5.3), we get

$$\mathrm{Im}(u)(1)=N(1)\simeq\mathrm{H}^1(G^{0+}(\overline{K}),\mu_p)=\mathrm{Hom}(G^{0+}(\overline{K}),\mu_p(\overline{K})). \tag{5.5.7}$$

This proves statement (ii) of the proposition.

Statement (iii) for $a=0$ has been proved above. Since the filtration G^a is decreasing and $\mathrm{U}^0G^\vee(\overline{K})=G^\vee(\overline{K})$, we may assume, for the proof of (iii), that $0<a\leq e'$. It suffices to prove that, under the pairing (5.5.3), we have

$$G^{a+}(\overline{K})^\perp=\mathrm{Im}(u)(1)\cap\mathrm{H}^0(B_s,\mathrm{U}^{e'-a}\Psi^1_B).$$

From (5.5.6) and (5.5.7), we check easily that (5.5.3) is identified with the canonical pairing

$$G^{0+}(\overline{K})\times\mathrm{H}^1(G^{0+}(\overline{K}),\mu_p)\to\mu_p(\overline{K}).$$

Hence we are reduced to prove that, under this pairing, we have

$$G^{a+}(\overline{K})^\perp=\mathrm{H}^1(G^{0+}(\overline{K}),\mu_p)\cap\mathrm{H}^0(B_s,\mathrm{U}^{e'-a}\Psi^1_B), \tag{5.5.8}$$

where the "$\cap$" is taken in $\mathrm{H}^1(\mathrm{Spec}\,L^{ur},\mu_p)$ (5.5.6).

Let $h:(L^{ur})^\times\to H^1(\mathrm{Spec}\,L^{ur},\mu_p)$ be the symbol morphism. We define a decreasing filtration on $\mathrm{H}^1(\mathrm{Spec}\,L^{ur},\mu_p)$ in a similar way as (3.2.2) by

$$\mathrm{U}^0\mathrm{H}^1=\mathrm{H}^1,\quad\text{and}\quad\mathrm{U}^b\mathrm{H}^1=h(1+\pi^b(\widehat{\mathcal{O}}_\mu)^{\mathrm{h}}_{\overline{\mu}})\text{ for all integers }b>0.$$

We extend this definition to all $b\in\mathbb{Q}_{\geq0}$ by setting $\mathrm{U}^b\mathrm{H}^1=\mathrm{U}^{[b]}\mathrm{H}^1$, where $[b]$ denotes the integer part of b. By ([1] Lemme 3.1.3), for all $b\in\mathbb{Q}_{>0}$, we have $\mathrm{H}^0(B_s,\mathrm{U}^b\Psi^1_B)=\rho_B^{-1}\Big(\mathrm{U}^b\mathrm{H}^1(\mathrm{Spec}\,L^{ur},\mu_p)\Big)$. Therefore, the right hand side of (5.5.8) is

$$\mathrm{H}^1(G^{0+}(\overline{K}),\mu_p)\cap\mathrm{U}^{(e'-a)}\mathrm{H}^1(\mathrm{Spec}\,L^{ur},\mu_p). \tag{5.5.9}$$

We identify $\mathrm{H}^1(G^{0+}(\overline{K}),\mu_p)$ with the character group $\mathrm{Hom}(\mathrm{Gal}(M^{ur}/L^{ur}),\mu_p(\overline{K}))$; then by ([1] Prop. 2.2.1), the subgroup (5.5.9) consists of the characters χ such that $\chi(\mathrm{Gal}(M^{ur}/L^{ur})^{(e'-a)+})=0$. In view of (5.5.5), we obtain immediately (5.5.8), which completes the proof.

□

Remark 5.6. The proof of 5.5(iii) follows the same strategy as the proof of ([1] Théorem 3.1.2). The referee point out that we can also reduce 5.5(iii) to 3.3. Indeed, the commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & G \arrow[r] \arrow[d, "\times p"] & A \arrow[r] \arrow[d, "\times p"] & B \arrow[r] \arrow[d, "\times p"] & 0 \\ 0 \arrow[r] & G \arrow[r] & A \arrow[r] & B \arrow[r] & 0 \end{tikzcd}$$

induces, by snake lemma, an exact sequence of finite group schemes $0 \to G \to {}_pA \xrightarrow{\phi} {}_pB \xrightarrow{\psi} G \to 0$. We consider the following perfect pairing

$$\begin{tikzcd} & {}_pA(\overline{K}) \arrow[d, "\phi"'] & {}_pA(\overline{K}) \times \mathrm{H}^1(A_{\overline{\eta}}, \mathbb{F}_p) \arrow[r, "(\bullet,\bullet)_A"] & \mathbb{F}_p \arrow[d, equal] & \mathrm{H}^1(A_{\overline{\eta}}, \mathbb{F}_p) \\ {}_pB^{a+}(\overline{K}) \arrow[r, hook] \arrow[d] & {}_pB(\overline{K}) \arrow[d, "\psi"'] & {}_pB(\overline{K}) \times \mathrm{H}^1(B_{\overline{\eta}}, \mathbb{F}_p) \arrow[r, "(\bullet,\bullet)_B"] & \mathbb{F}_p \arrow[d, equal] & \mathrm{H}^1(B_{\eta}, \mathbb{F}_p) \arrow[u, "\alpha_2"'] \\ G^{a+}(\overline{K}) \arrow[r, hook] & G(\overline{K}) & G(\overline{K}) \times G^{\vee}(\overline{K})(-1) \arrow[r, "(\bullet,\bullet)_G"] & \mathbb{F}_p & G^{\vee}(\overline{K}). \arrow[u, hook, "\gamma_2"'] \end{tikzcd}$$

By functoriality, the homomorphism ϕ is adjoint to α_2 and ψ is adjoint to γ_2, *i.e.* we have $(\phi(x), f)_B = (x, \alpha_2(f))_A$ and $(\psi(y), g)_B = (y, \gamma_2(g))_G$, for all $x \in {}_pA(\overline{K})$, $y \in {}_pB(\overline{K})$, $f \in \mathrm{H}^1(B_{\overline{\eta}}, \mathbb{F}_p)$ and $g \in G^{\vee}(\overline{K})$. By 2.8(ii), ψ induces a surjective homomorphism ${}_pB^{a+}(\overline{K}) \to G^{a+}(\overline{K})$ for all $a \in \mathbb{Q}_{\geq 0}$. Now statement 5.5(iii) follows from (5.4.1) and Theorem 3.3 applied to B.

6. Proof of Theorem 1.4(i)

6.1. For $r \in \mathbb{Q}_{>0}$, we denote by $\mathbb{G}_{a,r}$ the additive group scheme over $\overline{S}_r$ (1.9). Putting $t = 1-1/p$, we identify $\mathbb{G}_{a,t}$ with an abelian fppf-sheaf over $\overline{S}_1$ by the canonical immersion $i : \overline{S}_t \to \overline{S}_1$. Let $\mathrm{F} : \mathbb{G}_{a,1} \to \mathbb{G}_{a,1}$ be the Frobenius homomorphism, and c a p-th root of $(-p)$. It is easy to check that the morphism $\mathrm{F} - c : \mathbb{G}_{a,1} \to \mathbb{G}_{a,1}$, whose cokernel is denoted by $\mathbb{P}$, factorizes through the canonical reduction morphism $\mathbb{G}_{a,1} \to \mathbb{G}_{a,t}$, and we have an exact sequence of abelian fppf-sheaves on $\overline{S}_1$.

$$0 \to \mathbb{F}_p \to \mathbb{G}_{a,t} \xrightarrow{\mathrm{F}-c} \mathbb{G}_{a,1} \to \mathbb{P} \to 0. \tag{6.1.1}$$

This exact sequence gives (3.10.1) after restriction to the small étale topos $(\overline{X}_1)_{\text{ét}}$ for a smooth S-scheme X.

Proposition 6.2. *Assume $p \geq 3$. Let G be a truncated Barsotti-Tate group of level 1 over S, and $t = 1 - 1/p$. Then we have the equality*

$$\dim_{\mathbb{F}_p} \mathrm{U}^e G^{\vee}(\overline{K}) = \dim_{\mathbb{F}_p} \mathrm{Ker}\Big(\mathrm{Lie}(\overline{G}_t^{\vee}) \xrightarrow{\mathrm{F}-c} \mathrm{Lie}(\overline{G}_1^{\vee})\Big),$$

where $\mathrm{U}^e G^{\vee}(\overline{K})$ is the Bloch-Kato filtration (5.4), and the morphism in the right hand side is obtained by applying the functor $\mathrm{Hom}_{\overline{S}_1}(\overline{G}_1, \_)$ to the map $\mathrm{F} - c : \mathbb{G}_{a,t} \to \mathbb{G}_{a,1}$.

6.3. Before proving this proposition, we deduce first Theorem 1.4(i). Let G be a truncated Barsotti-Tate group of level 1 and height h over S satisfying the assumptions of 1.4, d be the dimension of $\mathrm{Lie}(G_s^\vee)$ over k, and $d^* = h - d$. It follows from 5.5(iii) and 6.2 that

$$\dim_{\mathbb{F}_p} G^{\frac{e}{p-1}+}(\overline{K}) = h - \dim_{\mathbb{F}_p} \mathrm{Ker}\Big(\mathrm{Lie}(\overline{G}_t^\vee) \xrightarrow{\mathrm{F}-c} \mathrm{Lie}(\overline{G}_1^\vee)\Big).$$

Since $\mathrm{Lie}(\overline{G}_1^\vee)$ is a free $\mathcal{O}_{\overline{S}_1}$-module of rank d^*, we obtain immediately Theorem 1.4(i) by applying Proposition 3.12 to $\lambda = c$ and $M = \mathrm{Lie}(\overline{G}_1^\vee)$.

The rest of this section is dedicated to the proof of Proposition 6.2.

Lemma 6.4. *Let G be a Barsotti-Tate group of level 1 over S, $t = 1 - \frac{1}{p}$. Then the morphism $\phi : \mathrm{Ext}^1(\overline{G}_1, \mathbb{F}_p) \to \mathrm{Ext}^1(\overline{G}_1, \mathbb{G}_{a,t})$ induced by the morphism $\mathbb{F}_p \to \mathbb{G}_{a,t}$ in* (6.1.1) *is injective.*

Proof. By ([12] Théorème 4.4(e)), there exists a Barsotti-Tate group H over S such that we have an exact sequence $0 \to G \to H \xrightarrow{\times p} H \to 0$, which induces a long exact sequence

$$\mathrm{Ext}^1(\overline{H}_1, \mathbb{F}_p) \xrightarrow{\times p} \mathrm{Ext}^1(\overline{H}_1, \mathbb{F}_p) \to \mathrm{Ext}^1(\overline{G}_1, \mathbb{F}_p) \to \mathrm{Ext}^2(\overline{H}_1, \mathbb{F}_p).$$

It is clear that the multiplication by p on $\mathrm{Ext}^1(\overline{H}_1, \mathbb{F}_p)$ is 0, and $\mathrm{Ext}^2(\overline{H}_1, \mathbb{F}_p) = 0$ by Corollary 4.9; hence the middle morphism in the exact sequence above is an isomorphism. Similarly, using $\mathrm{Ext}^2(\overline{H}_1, \mathbb{G}_{a,t}) = 0$ ([5] 3.3.2), we prove that the natural map $\mathrm{Ext}^1(\overline{H}_1, \mathbb{G}_{a,t}) \to \mathrm{Ext}^1(\overline{G}_1, \mathbb{G}_{a,t})$ is an isomorphism. So we get a commutative diagram

$$\begin{tikzcd}
\mathrm{Ext}^1(\overline{H}_1, \mathbb{F}_p) \arrow[r] \arrow[d, "\phi_H"] & \mathrm{Ext}^1(\overline{G}_1, \mathbb{F}_p) \arrow[d, "\phi"] \\
\mathrm{Ext}^1(\overline{H}_1, \mathbb{G}_{a,t}) \arrow[r] & \mathrm{Ext}^1(\overline{G}_1, \mathbb{G}_{a,t}),
\end{tikzcd}$$

where the horizontal maps are isomorphisms. Now it suffices to prove that ϕ_H is injective.

Let $\mathbb{K}$ be the fppf-sheaf on $\overline{S}_1$ determined by the following exact sequences:

$$0 \to \mathbb{F}_p \to \mathbb{G}_{a,t} \to \mathbb{K} \to 0; \quad 0 \to \mathbb{K} \to \mathbb{G}_{a,1} \to \mathbb{P} \to 0.$$

Applying the functors $\mathrm{Ext}^q(\overline{H}_1, \_)$, we get

$$\mathrm{Hom}(\overline{H}_1, \mathbb{K}) \to \mathrm{Ext}^1(\overline{H}_1, \mathbb{F}_p) \xrightarrow{\phi_H} \mathrm{Ext}^1(\overline{H}_1, \mathbb{G}_{a,t});$$
$$0 \to \mathrm{Hom}(\overline{H}_1, \mathbb{K}) \to \mathrm{Hom}(\overline{H}_1, \mathbb{G}_{a,1}) \to \mathrm{Hom}(\overline{H}_1, \mathbb{P}).$$

Since $\mathrm{Hom}(\overline{H}_1, \mathbb{G}_{a,1}) = 0$ ([5] 3.3.2), the injectivity of ϕ_H follows immediately. $\square$

6.5. Assume that $p \geq 3$. Let G be a commutative finite and flat group scheme killed by p over S, and $0 \to G \to A \to B \to 0$ be a resolution of G by abelian schemes (5.1.1). We denote $\mathcal{P}(B) = \mathrm{Coker}(\mathcal{O}_{\overline{B}_1} \xrightarrow{\mathrm{F}-c} \mathcal{O}_{\overline{B}_1})$ (3.7.1), and similarly for $\mathcal{P}(A)$. According to Remark 3.9, we have an identification

$$\mathrm{H}^0(B_{\overline{s}}, \mathrm{U}^e\Psi_B^1) \simeq \mathrm{H}^0(B_{\overline{s}}, \mathcal{P}(B)) = \mathrm{H}^0(\overline{B}_1, \mathcal{P}(B)) \tag{6.5.1}$$

as submodules of $\mathrm{H}^0(B_{\overline{s}}, \Psi^1_B)$; in the last equality, we have identified the topos $(B_{\overline{s}})_{\text{ét}}$ with $(\overline{B}_1)_{\text{ét}}$. We denote

$$\begin{aligned}\mathrm{Ker}(B, \mathrm{F}-c) &= \mathrm{Ker}\Big(\mathrm{H}^1(\overline{B}_1, \mathbb{G}_{a,t}) \xrightarrow{\mathrm{F}-c} \mathrm{H}^1(\overline{B}_1, \mathbb{G}_{a,1})\Big)\\ &= \mathrm{Ker}\Big(\mathrm{Lie}(\overline{B}^\vee_t) \xrightarrow{\mathrm{F}-c} \mathrm{Lie}(\overline{B}^\vee_1)\Big),\\ \mathrm{Ker}(B, \delta_E) &= \mathrm{Ker}\Big(\mathrm{H}^0(\overline{B}_1, \mathcal{P}(B)) \xrightarrow{\delta_E} \mathrm{H}^2(B_{\overline{s}}, \mathbb{F}_p)\Big),\end{aligned}$$

where δ_E is the morphism defined in Proposition 3.10(2); we have also similar notations for A. Since the exact sequence (3.10.2) is functorial in X, we have a commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{H}^1(B_{\overline{s}}, \mathbb{F}_p) \arrow[r] \arrow[d, "\beta_1"] & \mathrm{Ker}(B, \mathrm{F}-c) \arrow[r] \arrow[d, "\beta_2"] & \mathrm{Ker}(B, \delta_E) \arrow[r] \arrow[d, "\beta_3"] & 0 \\ 0 \arrow[r] & \mathrm{H}^1(A_{\overline{s}}, \mathbb{F}_p) \arrow[r] & \mathrm{Ker}(A, \mathrm{F}-c) \arrow[r] & \mathrm{Ker}(A, \delta_E) \arrow[r] & 0. \end{tikzcd} \tag{6.5.2}$$

Lemma 6.6. *The assumptions are those of* (6.5).

(i) *In diagram* (6.5.2)*, we have*

$$\mathrm{Ker}\,\beta_1 = \mathrm{Ker}\Big(\mathrm{Ext}^1(B_{\overline{s}}, \mathbb{F}_p) \to \mathrm{Ext}^1(A_{\overline{s}}, \mathbb{F}_p)\Big) = (G_{\text{ét}})^\vee(\overline{K})(-1); \tag{6.6.1}$$

$$\mathrm{Ker}\,\beta_2 = \mathrm{Ker}\Big(\mathrm{Lie}(\overline{G}^\vee_t) \xrightarrow{\mathrm{F}-c} \mathrm{Lie}(\overline{G}^\vee_1)\Big); \tag{6.6.2}$$

$$\mathrm{Ker}\,\beta_3 = \mathrm{H}^0(B_{\overline{s}}, \mathcal{P}(B)) \cap N(1) \subset \mathrm{H}^0(B_{\overline{s}}, \Psi^1_B), \tag{6.6.3}$$

where $N(1)$ is defined in (5.3.1).

(ii) *We have the equality*

$$\dim_{\mathbb{F}_p} \mathrm{U}^e G^\vee(\overline{K}) = \dim_{\mathbb{F}_p} \mathrm{Ker}\,\beta_1 + \dim_{\mathbb{F}_p} \mathrm{Ker}\,\beta_3. \tag{6.6.4}$$

In particular, we have

$$\dim_{\mathbb{F}_p} \mathrm{U}^e G^\vee(\overline{K}) \geq \dim_{\mathbb{F}_p} \mathrm{Ker}\Big(\mathrm{Lie}(\overline{G}^\vee_t) \xrightarrow{\mathrm{F}-c} \mathrm{Lie}(\overline{G}^\vee_1)\Big), \tag{6.6.5}$$

Moreover, the equality holds in (6.6.5) *if and only if the morphism* $\mathrm{Coker}\,\beta_1 \to \mathrm{Coker}\,\beta_2$ *induced by diagram* (6.5.2) *is injective.*

Proof. (i) By Corollary 4.6, we have a canonical isomorphism $\mathrm{Ext}^1(X_{\overline{s}}, \mathbb{F}_p) \simeq \mathrm{H}^1(X_{\overline{s}}, \mathbb{F}_p)$ for $X = A$ or B. Hence formula (6.6.1) follows easily by applying the functors $\mathrm{Ext}^q(\_, \mathbb{F}_p)$ to the exact sequence $0 \to G_{\overline{s}} \to A_{\overline{s}} \to B_{\overline{s}} \to 0$. Applying the morphism of functors $\mathrm{F}-c : \mathrm{Ext}^i(\_, \mathbb{G}_{a,t}) \to \mathrm{Ext}^i(\_, \mathbb{G}_{a,1})$ to the exact sequence $0 \to G \to A \to B \to 0$, we obtain the following commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{Lie}(\overline{G}^\vee_t) \arrow[r] \arrow[d, "\mathrm{F}-c"] & \mathrm{Lie}(\overline{B}^\vee_t) \arrow[r] \arrow[d, "\mathrm{F}-c"] & \mathrm{Lie}(\overline{A}^\vee_t) \arrow[d, "\mathrm{F}-c"] \\ 0 \arrow[r] & \mathrm{Lie}(\overline{G}^\vee_1) \arrow[r] & \mathrm{Lie}(\overline{B}^\vee_1) \arrow[r] & \mathrm{Lie}(\overline{A}^\vee_1) \end{tikzcd},$$

where we have used (4.7.1) and (4.7.2). Formula (6.6.2) follows immediately from this diagram. For (6.6.3), using (6.5.1), we have a commutative diagram

$$\begin{tikzcd}
\mathrm{Ker}(B,\delta_E) \arrow[r, "(1)"] \arrow[d, "\beta_3"'] & \mathrm{H}^0(B_{\overline{s}},\Psi^1_B) \arrow[d] \\
\mathrm{Ker}(A,\delta_E) \arrow[r, "(2)"] & \mathrm{H}^0(A_{\overline{s}},\Psi^1_A),
\end{tikzcd}$$

where the maps (1) and (2) are injective. Hence we obtain

$$\begin{aligned}
\mathrm{Ker}\,\beta_3 &= \mathrm{Ker}(B,\delta_E)\cap \mathrm{Ker}\Big(\mathrm{H}^0(B_{\overline{s}},\Psi^1(B))\to \mathrm{H}^0(A_{\overline{s}},\Psi^1(A))\Big)\\
&= \mathrm{Ker}(B,\delta_E)\cap N(1).
\end{aligned}$$

The morphisms δ_E and $d_2^{1,0}$ are compatible in the sense of Proposition 3.10, and Proposition 5.5 implies that $\mathrm{Ker}(B,\delta_E)\cap N(1)=\mathrm{H}^0(B_{\overline{s}},\mathcal{P}(B))\cap N(1)$, which proves (6.6.3).

(ii) By the isomorphism (5.5.1) and the surjectivity of the morphism u in (5.3.1), we have

$$\begin{aligned}
\dim_{\mathbb{F}_p}\mathrm{U}^eG^\vee(\overline{K}) &= \dim_{\mathbb{F}_p}\Big(G^\vee(\overline{K})(-1)\cap \mathrm{U}^e\mathrm{H}^1(B_{\overline{\eta}},\mathbb{Z}/p\mathbb{Z})\Big)\\
&= \dim_{\mathbb{F}_p}\Big((G_{\text{ét}})^\vee(\overline{K})(-1)\Big)+\dim_{\mathbb{F}_p}\Big(N\cap \mathrm{H}^0(B_{\overline{s}},\mathrm{U}^e\Psi^1(B))(-1)\Big). \qquad (6.6.6)
\end{aligned}$$

Then the equality (6.6.4) follows from (i) of this lemma and (6.5.1). The rest part of (ii) follows immediately from diagram (6.5.2). □

6.7. ***Proof of Proposition 6.2.*** We choose a resolution $0\to G\to A\to B\to 0$ of G by abelian schemes (5.1.1). By Lemma 6.6, we have to prove that if G is a truncated Barsotti-Tate group of level 1 over S, the morphism $\phi_{12}:\mathrm{Coker}\,\beta_1\to\mathrm{Coker}\,\beta_2$ induced by diagram (6.5.2) is injective.

By 4.6, we have $\mathrm{H}^1_{\text{ét}}(X_{\overline{s}},\mathbb{F}_p)=\mathrm{H}^1_{\text{ét}}(\overline{X}_1,\mathbb{F}_p)=\mathrm{Ext}^1(\overline{X}_1,\mathbb{F}_p)$ for $X=A$ or B. Thus the morphism β_1 is canonically identified to the morphism $\mathrm{Ext}^1(\overline{B}_1,\mathbb{F}_p)\to\mathrm{Ext}^1(\overline{A}_1,\mathbb{F}_p)$ induced by the map $A\to B$. Applying the functors $\mathrm{Ext}^i(\_,\mathbb{F}_p)$ to $0\to\overline{G}_1\to\overline{A}_1\to\overline{B}_1\to 0$, we obtain a long exact sequence

$$\mathrm{Ext}^1(\overline{B}_1,\mathbb{F}_p)\to\mathrm{Ext}^1(\overline{A}_1,\mathbb{F}_p)\to\mathrm{Ext}^1(\overline{G}_1,\mathbb{F}_p)\to\mathrm{Ext}^2(\overline{B}_1,\mathbb{F}_p).$$

Since $\mathrm{Ext}^2(\overline{B}_1,\mathbb{F}_p)=0$ by 4.9, we have $\mathrm{Coker}\,\beta_1=\mathrm{Ext}^1(\overline{G}_1,\mathbb{F}_p)$. The commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Ker}(B,\mathrm{F}-c) \arrow[r] \arrow[d, "\beta_2"'] & \mathrm{Lie}(B_t^\vee) \arrow[r, "\mathrm{F}-c"] \arrow[d, "\gamma"'] & \mathrm{Lie}(B_1^\vee) \arrow[d] \\
0 \arrow[r] & \mathrm{Ker}(A,\mathrm{F}-c) \arrow[r] & \mathrm{Lie}(A_t^\vee) \arrow[r, "\mathrm{F}-c"] & \mathrm{Lie}(A_1^\vee),
\end{tikzcd}$$

induces a canonical morphism $\psi:\mathrm{Coker}\,\beta_2\to\mathrm{Coker}\,\gamma=\mathrm{Ext}^1(\overline{G}_1,\mathbb{G}_{a,t})$. Let $\phi:\mathrm{Ext}^1(\overline{G}_1,\mathbb{F}_p)\to\mathrm{Ext}^1(\overline{G}_1,\mathbb{G}_{a,t})$ be the morphism induced by the map $\mathbb{F}_p\to\mathbb{G}_{a,t}$ in (6.1.1). Then we have the following commutative diagram

$$\begin{tikzcd}
\mathrm{Ext}^1(\overline{G}_1,\mathbb{F}_p)=\mathrm{Coker}\,\beta_1 \arrow[r, "\phi_{12}"] \arrow[dr, "\phi"'] & \mathrm{Coker}\,\beta_2 \arrow[d, "\psi"] \\
& \mathrm{Ext}^1(\overline{G}_1,\mathbb{G}_{a,t}).
\end{tikzcd}$$

Now Lemma 6.4 implies that ϕ is injective, hence so is ϕ_{12}. This completes the proof.

7. The canonical filtration in terms of congruence groups

7.1. Recall the following definitions in [20]. For any $\lambda \in \mathcal{O}_{\overline{K}}$, let $\mathcal{G}^{(\lambda)}$ be the group scheme $\mathrm{Spec}(\mathcal{O}_{\overline{K}}[T, \frac{1}{1+\lambda T}])$ with the comultiplication given by $T \mapsto T\otimes 1 + 1\otimes T + \lambda T\otimes T$, the counit by $T=0$ and the coinverse by $T\mapsto -\frac{T}{1+\lambda T}$. If $v(\lambda)\leq e/(p-1)$, we put

$$P_\lambda(T) = \frac{(1+\lambda T)^p - 1}{\lambda^p} \in \mathcal{O}_{\overline{K}}[T]$$

and let $\phi_\lambda : \mathcal{G}^{(\lambda)} \to \mathcal{G}^{(\lambda^p)}$ be the morphism of $\mathcal{O}_{\overline{K}}$-group schemes defined on the level of Hopf algebras by $T\mapsto P_\lambda(T)$. We denote by G_λ the kernel of ϕ_λ, so we have $G_\lambda = \mathrm{Spec}\big(\mathcal{O}_{\overline{K}}[T]/P_\lambda(T)\big)$. We call it, following Raynaud, the *congruence group of level* λ. It is a finite flat group scheme over $\overline{S} = \mathrm{Spec}(\mathcal{O}_{\overline{K}})$ of rank p.

7.2. For all $\lambda \in \mathcal{O}_{\overline{K}}$ with $v(\lambda)\leq e/(p-1)$, let $\theta_\lambda : G_\lambda \to \mu_p = \mathrm{Spec}(\mathcal{O}_{\overline{K}}[X]/(X^p-1))$ be the homomorphism given on the level of Hopf algebras by $X\mapsto 1+\lambda T$. Then $\theta_\lambda \otimes \overline{K}$ is an isomorphism, and if $v(\lambda)=0$, θ_λ is an isomorphism. For all $\lambda,\gamma\in\mathcal{O}_{\overline{K}}$ with $v(\gamma)\leq v(\lambda)\leq e/(p-1)$, let $\theta_{\lambda,\gamma} : G_\lambda \to G_\gamma$ be the map defined by the homomorphism of Hopf algebras $T\mapsto (\lambda/\gamma)T$. We have $\theta_\lambda = \theta_\gamma\circ\theta_{\lambda,\gamma}$.

7.3. Let $\lambda\in\mathcal{O}_{\overline{K}}$ with $v(\lambda)\leq e/(p-1)$, A be an abelian scheme over S. We define

$$\theta_\lambda(A) : \mathrm{Ext}^1_{\overline{S}}(A, G_\lambda) \to \mathrm{Ext}^1_{\overline{S}}(A,\mu_p) \tag{7.3.1}$$

to be the homomorphism induced by the canonical morphism $\theta_\lambda : G_\lambda\to\mu_p$, where, by abuse of notations, A denotes also the inverse image of A over $\overline{S}$, and $\mathrm{Ext}^1_{\overline{S}}$ means the extension in the category of abelian fppf-sheaves over $\overline{S}$. Similarly, let G be a commutative finite and flat group scheme killed by p over S; we define

$$\theta_\lambda(G) : \mathrm{Hom}_{\overline{S}}(G, G_\lambda) \to \mathrm{Hom}_{\overline{S}}(G,\mu_p) = G^\vee(\overline{K}) \tag{7.3.2}$$

to be the homomorphism induced by θ_λ. If $G = {}_pA$, where A is an S-abelian scheme, the natural exact sequence $0\to {}_pA \to A \xrightarrow{\times p} A \to 0$ induces a commutative diagram

$$\begin{tikzcd} \mathrm{Hom}_{\overline{S}}({}_pA, G_\lambda) \arrow[r] \arrow[d, "\theta_\lambda({}_pA)"'] & \mathrm{Ext}^1_{\overline{S}}(A, G_\lambda) \arrow[d, "\theta_\lambda(A)"] \\ {}_pA^\vee(\overline{K}) \arrow[r] & \mathrm{Ext}^1_{\overline{S}}(A,\mu_p), \end{tikzcd} \tag{7.3.3}$$

where horizontal maps are isomorphisms (4.3.2). Hence, $\theta_\lambda(A)$ is canonically identified to $\theta_\lambda({}_pA)$.

Lemma 7.4. *Let $\lambda,\gamma\in\mathcal{O}_{\overline{K}}$ with $v(\gamma)\leq v(\lambda)\leq e/(p-1)$, G be a commutative finite and flat group scheme killed by p over S.*

(i) *$\theta_\lambda(G)$ is injective.*

(ii) *The image of $\theta_\lambda(G)$ is contained in that of $\theta_\gamma(G)$.*

(iii) *The image of $\theta_\lambda(G)$ depends only on $v(\lambda)$, and it is invariant under the action of the Galois group* $\mathrm{Gal}(\overline{K}/K)$.

Proof. We have a commutative diagram

$$\begin{tikzcd} \mathrm{Hom}_{\overline{S}}(G_\lambda^\vee, G^\vee) \arrow[r, "\theta_\lambda(G)"] \arrow[d, "(1)"'] & \mathrm{Hom}_{\overline{S}}(\mathbb{Z}/p\mathbb{Z}, G^\vee) \arrow[d, equal] \\ \mathrm{Hom}_{\overline{\eta}}(G_\lambda^\vee, G^\vee) \arrow[r, "(2)"] & \mathrm{Hom}_{\overline{\eta}}(\mathbb{Z}/p\mathbb{Z}, G^\vee), \end{tikzcd} \tag{7.4.1}$$

where the horizontal maps are induced by $\theta_\lambda^\vee : \mathbb{Z}/p\mathbb{Z} \to G_\lambda^\vee$, and the vertical maps are induced by the base change $\overline{\eta} \to \overline{S}$. Since θ_λ is an isomorphism over the generic point (7.2), the map (2) is an isomorphism. Hence statement (i) follows from the fact that (1) is injective by the flatness of G and G_λ.

Statement (ii) follows easily from the existence of the morphism $\theta_{\lambda,\gamma} : G_\lambda \to G_\gamma$ with $\theta_\lambda = \theta_\gamma \circ \theta_{\lambda,\gamma}$. The first part of (iii) follows immediately from (ii). Any $\sigma \in \mathrm{Gal}(\overline{K}/K)$ sends the image of $\theta_\lambda(G)$ isomorphically to the image of $\theta_{\sigma(\lambda)}(G)$, which coincides with the former by the first assertion of (iii). □

7.5. **Filtration by congruence groups.** Let a be a rational number with $0 \leq a \leq e/(p-1)$, and G be a commutative finite and flat group scheme over S killed by p. We choose $\lambda \in \mathcal{O}_{\overline{K}}$ with $v(\lambda) = a$, and denote by $G^\vee(\overline{K})^{[a]}$ the image of $\theta_\lambda(G)$. By Lemma 7.4, $G^\vee(\overline{K})^{[a]}$ depends only on a, and not on the choice of λ. Then $\big(G^\vee(\overline{K})^{[a]}, a \in \mathbb{Q} \cap [0, e/(p-1)]\big)$ is an exhaustive decreasing filtration of $G^\vee(\overline{K})$ by $\mathrm{Gal}(\overline{K}/K)$-groups.

7.6. Let $\lambda \in \mathcal{O}_{\overline{K}}$ with $0 \leq v(\lambda) \leq e/(p-1)$, $f : A \to S$ be an abelian scheme, and $\overline{f} : \overline{A} \to \overline{S}$ its base change by $\overline{S} \to S$. In ([3] §6), Andreatta and Gasbarri consider the homomorphism $\theta'_\lambda(A) : \mathrm{H}^1_{\mathrm{fppf}}(\overline{A}, G_\lambda) \to \mathrm{H}^1_{\mathrm{fppf}}(\overline{A}, \mu_p)$ induced by θ_λ, where by abuse of notation, G_λ denotes also the fppf-sheaf G_λ restricted to $\overline{A}$. We have a commutative diagram

$$\begin{tikzcd} \mathrm{Ext}^1_{\overline{S}}(A, G_\lambda) \arrow[r, "\varphi(G_\lambda)"] \arrow[d, "\theta_\lambda(A)"'] & \mathrm{H}^1_{\mathrm{fppf}}(\overline{A}, G_\lambda) \arrow[d, "\theta'_\lambda(A)"] \\ \mathrm{Ext}^1_{\overline{S}}(A, \mu_p) \arrow[r, "\varphi(\mu_p)"] & \mathrm{H}^1_{\mathrm{fppf}}(\overline{A}, \mu_p), \end{tikzcd} \tag{7.6.1}$$

where the horizontal arrows are the homomorphisms (4.4.1).

Lemma 7.7. (i) *The homomorphisms $\varphi(G_\lambda)$ and $\varphi(\mu_p)$ in* (7.6.1) *are isomorphisms. In particular, the homomorphism $\theta'_\lambda(A)$ is canonically isomorphic to $\theta_\lambda(A)$* (7.3.1).

(ii) *The canonical morphism $\mathrm{H}^1_{\mathrm{fppf}}(\overline{A}, \mu_p) \to \mathrm{H}^1(A_{\overline{\eta}}, \mu_p)$ is an isomorphism. Let $\mathrm{H}^1(A_{\overline{\eta}}, \mu_p)^{[v(\lambda)]}$ be the image of $\theta'_\lambda(A)$ composed with this isomorphism. Then via the canonical isomorphism $\mathrm{H}^1(A_{\overline{\eta}}, \mu_p) \simeq {}_pA^\vee(\overline{K})$, the subgroup $\mathrm{H}^1(A_{\overline{\eta}}, \mu_p)^{[v(\lambda)]}$ is identified to ${}_pA^\vee(\overline{K})^{[v(\lambda)]}$.*

Proof. (i) For $H = G_\lambda$ or μ_p, the "local-global" spectral sequence induces an exact sequence

$$0 \to \mathrm{H}^1_{\mathrm{fppf}}(\overline{S}, R^0_{\mathrm{fppf}}\overline{f}_*(H_{\overline{A}})) \to \mathrm{H}^1_{\mathrm{fppf}}(\overline{A}, H_{\overline{A}}) \xrightarrow{\psi(H)} \mathrm{H}^0_{\mathrm{fppf}}(\overline{S}, R^1_{\mathrm{fppf}}\overline{f}_*(H_{\overline{A}})). \tag{7.7.1}$$

By Prop. 4.5 and (4.3.2), we have isomorphisms

$$\mathrm{H}^0_{\mathrm{fppf}}(\overline{S}, R^1_{\mathrm{fppf}}\overline{f}_*(H_{\overline{A}})) \simeq \mathrm{H}^0_{\mathrm{fppf}}(\overline{S}, \mathcal{E}xt^1_{\overline{S}}(A, H)) \simeq \mathrm{Ext}^1_{\overline{S}}(A, H).$$

Therefore, we obtain a homomorphism $\psi(H) : \mathrm{H}^1_{\mathrm{fppf}}(\overline{A}, H_{\overline{A}}) \to \mathrm{Ext}^1_{\overline{S}}(A, H)$. We check that the composed map $\psi(H) \circ \varphi(H)$ is the identity morphism on $\mathrm{Ext}^1_{\overline{S}}(A, H)$; in particular, $\psi(H)$ is

surjective. By Prop. 4.5, we have also $R^0_{\mathrm{fppf}}\overline{f}_*(H_{\overline{A}}) = H_{\overline{S}}$; on the other hand, it follows from ([3] Lemma 6.2) that $\mathrm{H}^1_{\mathrm{fppf}}(\overline{S}, H_{\overline{S}}) = 0$. Hence $\psi(H)$ is injective by the exact sequence (7.7.1), and $\varphi(H)$ and $\psi(H)$ are both isomorphisms.

(ii) We have a commutative diagram

$$\begin{tikzcd}
\mathrm{Ext}^1_{\overline{S}}(A, \mu_p) \arrow[r, "\varphi(\mu_p)"] \arrow[d, "(1)"'] & \mathrm{H}^1_{\mathrm{fppf}}(\overline{A}, \mu_p) \arrow[d, "(2)"] \\
\mathrm{Ext}^1_{\overline{\eta}}(A_{\overline{\eta}}, \mu_p) \arrow[r] & \mathrm{H}^1(A_{\overline{\eta}}, \mu_p),
\end{tikzcd}$$

where the vertical maps are base changes to the generic fibres, and the horizontal morphisms are (4.4.1), which are isomorphisms in our case by (4.6) and statement (i). The morphism (1) is easily checked to be an isomorphism using (4.3.2), hence so is the morphism (2). The second part of statement (ii) is a consequence of (i). □

The following proposition, together with Proposition 5.5, implies Theorem 1.6.

Proposition 7.8. *Let G be a commutative finite and flat group scheme over S killed by p. Then, for all rational numbers $0 \leq a \leq e/(p-1)$, we have $G^\vee(\overline{K})^{[a]} = \mathrm{U}^{pa}G^\vee(\overline{K})$, where $\mathrm{U}^\bullet G^\vee(\overline{K})$ is the Bloch-Kato filtration* (5.4).

Proof. Let $0 \to G \to A \to B \to 0$ be a resolution of G by abelian schemes (5.1.1). We have, for all $\lambda \in \mathcal{O}_{\overline{K}}$ with $0 \leq v(\lambda) \leq e/(p-1)$, a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Hom}_{\overline{S}}(G, G_\lambda) \arrow[r] \arrow[d, hook, "\theta_\lambda(G)"] & \mathrm{Ext}^1_{\overline{S}}(B, G_\lambda) \arrow[r] \arrow[d, hook, "\theta_\lambda(B)"] & \mathrm{Ext}^1_{\overline{S}}(A, G_\lambda) \arrow[d, hook, "\theta_\lambda(A)"] \\
0 \arrow[r] & G^\vee(\overline{K}) \arrow[r] & {}_pB^\vee(\overline{K}) \arrow[r] & {}_pA^\vee(\overline{K}).
\end{tikzcd}$$

Hence, for all rational numbers a satisfying $0 \leq a \leq e/(p-1)$, we have by 7.7(ii)

$$G^\vee(\overline{K})^{[a]} = G^\vee(\overline{K}) \cap {}_pB^\vee(\overline{K})^{[a]} = G^\vee(\overline{K}) \cap \mathrm{H}^1(B_{\overline{\eta}}, \mu_p)^{[a]}. \tag{7.8.1}$$

According to ([3] Theorem 6.8), the filtration $(\mathrm{H}^1(B_{\overline{\eta}}, \mu_p)^{[a]}, 0 \leq a \leq e/(p-1))$ coincides with the filtration $(\mathrm{U}^{pa}\mathrm{H}^1(B_{\overline{\eta}}, \mu_p), 0 \leq a \leq \frac{e}{p-1})$ (3.2.3). Hence by (7.8.1) and (5.4.1), the two filtrations $\big(G^\vee(\overline{K})^{[a]}\big)$ and $\big(\mathrm{U}^{pa}G^\vee(\overline{K})\big)$ on $G^\vee(\overline{K})$ coincide. This completes the proof.

□

8. The lifting property of the canonical subgroup

In this section, by abuse of notations, $\mathbb{G}_a$ will denote the additive group both over S and over $\overline{S}$. For a rational number $r > 0$, we denote by $\mathbb{G}_{a,r}$, $\mathcal{G}_r^{(\lambda)}$ and $G_{\lambda,r}$ the base changes to $\overline{S}_r$ of the respective group schemes.

8.1. Following [21], for $a, c \in \mathcal{O}_{\overline{K}}$ with $ac = p$, we denote by $G_{a,c}$ the group scheme $\mathrm{Spec}\big(\mathcal{O}_{\overline{K}}[y]/(y^p - ay)\big)$ over $\mathcal{O}_{\overline{K}}$ with comultiplication

$$y \mapsto y \otimes 1 + 1 \otimes y + \frac{cw_{p-1}}{1-p} \sum_{i=1}^{p-1} \frac{y^i}{w_i} \otimes \frac{y^{p-i}}{w_{p-i}}$$

and the counit given by $y = 0$, where w_i $(1 \leq i \leq p-1)$ are universal constants in $\mathcal{O}_{\overline{K}}$ with $v(w_i) = 0$ (see [21] p.9). Tate and Oort proved that $(a, c) \mapsto G_{a,c}$ gives a bijection between equivalence classes of factorizations of $p = ac$ in $\mathcal{O}_{\overline{K}}$ and isomorphism classes of $\mathcal{O}_{\overline{K}}$-group schemes of order p, where two factorizations $p = a_1c_1$ and $p = a_2c_2$ are called equivalent if there exists $u \in \mathcal{O}_{\overline{K}}$ such that $a_2 = u^{p-1}a_1$ and $c_2 = u^{1-p}c_1$.

Let $\lambda \in \mathcal{O}_{\overline{K}}$ with $0 \leq v_p(\lambda) \leq 1/(p-1)$. There exists a factorization $p = a(\lambda)c(\lambda)$ such that $G_\lambda \simeq G_{a(\lambda),c(\lambda)}$. More explicitly, we may take $c(\lambda) = \frac{(\lambda(1-p))^{p-1}}{w_{p-1}}$ and $a(\lambda) = \frac{p}{c(\lambda)}$, and we notice that $v_p(a(\lambda)) = 1 - (p-1)v_p(\lambda)$ is well defined independently of the factorization $p = a(\lambda)c(\lambda)$.

Lemma 8.2 ([3] Lemma 8.2 and 8.10)**.** *Let $0 < r \leq 1$ be a rational number and $\lambda \in \mathcal{O}_{\overline{K}}$ with $v_p(\lambda) \leq 1 - 1/p$ and $v_p(\lambda^{p-1}) \geq r$.*

(i) *Let ρ_r^λ be the morphism of groups schemes $\mathcal{G}_r^{(\lambda)} = \mathrm{Spec}\big(\mathcal{O}_{\overline{S}_t}[T]\big) \to \mathbb{G}_{a,r} = \mathrm{Spec}\big(\mathcal{O}_{\overline{S}_r}[X]\big)$ defined on the level of Hopf algebras by $X \mapsto \sum_{i=1}^{p-1}(-\lambda)^{i-1}\frac{T^i}{i}$. Then ρ_r^λ is an isomorphism. Moreover, the following diagram is commutative*

$$\begin{tikzcd}
\mathcal{G}_r^{(\lambda)} \arrow[r, "\phi_{\lambda,r}"] \arrow[d, "\rho_r^\lambda"'] & \mathcal{G}_r^{(\lambda^p)} \arrow[d, "\rho_r^{\lambda^p}"] \\
\mathbb{G}_{a,r} \arrow[r, "\mathrm{F}-a(\lambda)"] & \mathbb{G}_{a,r},
\end{tikzcd}$$

where F *is the Frobenius homomorphism and $a(\lambda) \in \mathcal{O}_{\overline{K}}$ is introduced in* (8.1)*.*

(ii) *Let $\delta_{\lambda,r}$ be the composed morphism $G_{\lambda,r} \xrightarrow{i} \mathcal{G}_r^{(\lambda)} \xrightarrow{\rho_r^\lambda} \mathbb{G}_{a,r}$. Then $\delta_{\lambda,r}$ generates* $\mathrm{Lie}(G_{\lambda,r}^\vee) \simeq \mathrm{Hom}_{\overline{S}_r}(G_{\lambda,r}, \mathbb{G}_{a,r})$ *as an $\mathcal{O}_{\overline{S}_r}$-module.*

Lemma 8.3 ([3] Lemma 8.3)**.** *Let $\lambda \in \mathcal{O}_{\overline{K}}$ with $\frac{1}{p(p-1)} \leq v_p(\lambda) \leq \frac{1}{p-1}$, and $r = (p-1)v_p(\lambda)$. Then the following diagram is commutative*

$$\begin{tikzcd}
\mathcal{G}_1^{(\lambda)} \arrow[rr, "\phi_{\lambda,1}"] \arrow[d, "\iota_{1,r}"'] & & \mathcal{G}_1^{(\lambda^p)} \arrow[d, "\rho_r^{\lambda^p}"] \\
\mathcal{G}_r^{(\lambda)} \arrow[r, "\rho_r^\lambda"] & \mathbb{G}_{a,r} \arrow[r, "\mathrm{F}-a(\lambda)"] & \mathbb{G}_{a,1},
\end{tikzcd}$$

where $\iota_{1,r}$ is the reduction map.

8.4. Let $\lambda \in \mathcal{O}_{\overline{K}}$ with $v_p(\lambda) = \frac{1}{p}$, $t = 1 - 1/p$, and G be a commutative finite and flat group scheme killed by p over S. We define Φ_G to be

(8.4.1) $$\Phi_G : \mathrm{Hom}_{\overline{S}}(\overline{G}, G_\lambda) \xrightarrow{\iota_t} \mathrm{Hom}_{\overline{S}_t}(\overline{G}_t, G_{\lambda,t}) \xrightarrow{\delta} \mathrm{Hom}_{\overline{S}_t}(\overline{G}_t, \mathbb{G}_{a,t}) = \mathrm{Lie}(\overline{G}_t^\vee),$$

where ι_t is the canonical reduction map, and δ is the morphism induced by the element $\delta_{\lambda,t} \in \mathrm{Hom}_{\overline{S}_t}(G_{\lambda,t}, \mathbb{G}_{a,t})$ (8.2(ii)).

Proposition 8.5. *Let $\lambda \in \mathcal{O}_{\overline{K}}$ with $v_p(\lambda) = \frac{1}{p}$, $t = 1 - 1/p$, and G be a a Barsotti-Tate group of level 1 over S, satisfying the hypothesis of Theorem 1.4. Then we have an exact sequence*

(8.5.1) $$0 \to \mathrm{Hom}_{\overline{S}}(\overline{G}, G_\lambda) \xrightarrow{\Phi_G} \mathrm{Hom}_{\overline{S}_t}(\overline{G}_t, \mathbb{G}_{a,t}) \xrightarrow{\mathrm{F}-a(\lambda)} \mathrm{Hom}_{\overline{S}_1}(\overline{G}_1, \mathbb{G}_{a,1}),$$

where $a(\lambda)$ is defined in 8.1.

Proof. From Lemma 8.3, we deduce a commutative diagram
(8.5.2)

$$\begin{tikzcd}
\mathrm{Hom}_{\overline{S}_1}(\overline{G}_1, G_{\lambda,1}) \arrow[r] \arrow[d, "\iota_{1,t}"'] & \mathrm{Hom}_{\overline{S}_1}(\overline{G}_1, \mathcal{G}_1^{(\lambda)}) \arrow[rr, "\phi_{\lambda,1}"] \arrow[d, "\iota'_{1,t}"'] & & \mathrm{Hom}_{\overline{S}_1}(\overline{G}_1, \mathcal{G}_1^{(\lambda^p)}) \arrow[d, "\rho_1^{\lambda^p}"] \\
\mathrm{Hom}_{\overline{S}_t}(\overline{G}_t, G_{\lambda,t}) \arrow[r] & \mathrm{Hom}_{\overline{S}_t}(\overline{G}_t, \mathcal{G}_t^{(\lambda)}) \arrow[r, "\rho_t^{\lambda}"] & \mathrm{Hom}_{\overline{S}_t}(\overline{G}_t, \mathbb{G}_{a,t}) \arrow[r, "\mathrm{F}-a(\lambda)"] & \mathrm{Hom}_{\overline{S}_1}(\overline{G}_1, \mathbb{G}_{a,1}),
\end{tikzcd}$$

where the upper row is exact and $\iota_{1,t}$ and $\iota'_{1,t}$ are reduction maps. Therefore, the composition of Φ_G with the morphism $\mathrm{F} - a(\lambda)$ in (8.5.1) factorizes through the upper row of (8.5.2), and equals thus 0. Let L be the kernel of the map $\mathrm{F} - a(\lambda)$ in (8.5.1). Then Φ_G induces a map $\Phi' : \mathrm{Hom}_{\overline{S}}(\overline{G}, G_\lambda) \to L$. We have to prove that Φ' is an isomorphism.

Let d^* be the rank of $\mathrm{Lie}(\overline{G}_1^\vee) = \mathrm{Hom}_{\overline{S}_1}(\overline{G}_1, \mathbb{G}_{a,1})$ over $\mathcal{O}_{\overline{S}_1}$, and recall that $v_p(a(\lambda)) = 1/p$. Since G satisfies the assumptions of Theorem 1.4, applying Prop. 3.12 to $\mathrm{Lie}(\overline{G}_1^\vee)$ and the operator $\mathrm{F} - a(\lambda)$, we see that the group L is an $\mathbb{F}_p$-vector space of dimension d^*. On the other hand, $\mathrm{Hom}_{\overline{S}}(\overline{G}, G_\lambda)$ is identified with $G^{\frac{e}{p-1}+}(\overline{K})^\perp$ by Theorem 1.6. Thus it is also an $\mathbb{F}_p$-vector space of dimension d^* by Theorem 1.4(i). Therefore, to finish the proof, it suffices to prove that Φ' is surjective.

By Lemma 8.2(i), we have the following commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & L \arrow[r] \arrow[d, "\alpha"'] & \mathrm{Hom}_{\overline{S}_t}(\overline{G}_t, \mathbb{G}_{a,t}) \arrow[r, "\mathrm{F}-a(\lambda)"] \arrow[d, equal] & \mathrm{Hom}_{\overline{S}_1}(\overline{G}_1, \mathbb{G}_{a,1}) \arrow[d, "\iota_{1,t}"] \\
0 \arrow[r] & \mathrm{Hom}_{\overline{S}_t}(\overline{G}_t, G_{\lambda,t}) \arrow[r] & \mathrm{Hom}_{\overline{S}_t}(\overline{G}_t, \mathbb{G}_{a,t}) \arrow[r, "\mathrm{F}-a(\lambda)"] & \mathrm{Hom}_{\overline{S}_t}(\overline{G}_t, \mathbb{G}_{a,t}),
\end{tikzcd}$$

where $\iota_{1,t}$ is the reduction map. The composed morphism $\alpha \circ \Phi'$ is the canonical reduction map, whose injectivity will implies the injectivity of Φ'. Thus the following lemma will conclude the proof of the proposition. $\square$

Lemma 8.6. *Assume that $p \geq 3$. Let $t = 1 - 1/p$, $\lambda \in \mathcal{O}_{\overline{K}}$ with $v_p(\lambda) = 1/p$, and G be a commutative finite flat group scheme killed by p over S. Then the reduction map*

$$\iota_t : \mathrm{Hom}_{\overline{S}}(\overline{G}, G_\lambda) \to \mathrm{Hom}_{\overline{S}_t}(\overline{G}_t, G_{\lambda,t})$$

is injective.

Proof. We put $G \times_S \overline{S} = \mathrm{Spec}(A)$, where A is a Hopf algebra over $\mathcal{O}_{\overline{K}}$ with the comultiplication Δ. An element $f \in \mathrm{Hom}_{\overline{S}}(\overline{G}, G_\lambda)$ is determined by an element $x \in A$ satisfying

$$\Delta(x) = x \otimes 1 + 1 \otimes x + \lambda x \otimes x$$

$$P_\lambda(x) = \frac{(1+\lambda x)^p - 1}{\lambda^p} = 0. \tag{8.6.1}$$

Suppose that $\iota_t(f) = 0$, which means $x \in \mathfrak{m}_t A$. We want to prove that in fact $x = 0$. Let us write $x = \lambda^a y$ where $a \geq p - 1 \geq 2$ is an integer, and $y \in A$. Substituting x in (8.6.1), we obtain

$$(\lambda^a y)^p + \sum_{i=1}^{p-1} \frac{1}{\lambda^p} \binom{p}{i} \lambda^{i(a+1)} y^i = 0.$$

Since $v_p(\frac{1}{\lambda^p}\binom{p}{i}) = 0$ for $1 \leq i \leq p-1$ and A is flat over $\mathcal{O}_K$, we see easily that $y = \lambda^{a+1} y_1$ for some $y_1 \in A$. Continuing this process, we find that $x \in \cap_{a \in \mathbb{Q}_{>0}} \mathfrak{m}_a A = 0$ (1.9). $\square$

Lemma 8.7. *Let G be a Barsotti-Tate group of level 1 and height h over S, and H be a flat closed subgroup scheme of G. We denote by d the dimension of $\mathrm{Lie}(G_s)$ over k, and $d^* = h - d$. Then the following conditions are equivalent:*

(i) *The special fiber H_s of H coincides with the kernel of the Frobenius of G_s.*
(i') *The special fiber $H_s^\perp$ of $H^\perp = (G/H)^\vee$ coincides with the kernel of the Frobenius of $G_s^\vee$.*
(ii) *H has rank p^d over S and $\dim_k \mathrm{Lie}(H_s) \geq d$.*
(ii') *$H^\perp$ has rank p^{d^*} over S and $\dim_k \mathrm{Lie}(H_s^\perp) \geq d^*$.*

Proof. We have two exact sequences

$$0 \to H \to G \to G/H \to 0$$
$$0 \to H^\perp \to G^\vee \to H^\vee \to 0.$$

Denote by $\mathfrak{F}_{G_s}$ (*resp.* by $\mathfrak{V}_{G_s}$) the Frobenius (*resp.* the Verschiebung) of G_s. Assume that (i) is satisfied, then we have $H_s^\vee = \mathrm{Coker}(\mathfrak{V}_{G_s^\vee})$ by duality. Since G is a Barsotti-Tate group of level 1, $H_s^\perp$ coincides with $\mathrm{Im}(\mathfrak{V}_{G_s^\vee}) = \mathrm{Ker}(\mathfrak{F}_{G_s^\vee})$. Conversely, if $H_s^\perp = \mathrm{Ker}(\mathfrak{F}_{G_s^\vee})$, we have also $H_s = \mathrm{Ker}(\mathfrak{F}_{G_s})$. This proves the equivalence of (i) and (i').

If (i) or (i') is satisfied, then (ii) and (ii') are also satisfied (SGA 3_1 $\mathrm{VII_A}$ 7.4). Assume (ii) satisfied. Since $\mathrm{Ker}(\mathfrak{F}_{H_s})$ has rank $p^{\dim_k \mathrm{Lie}(H_s)}$ (*loc. cit.*) and is contained in both $\mathrm{Ker}(\mathfrak{F}_{G_s})$ and H_s, condition (ii) implies that these three groups have the same rank; hence they coincide. This proves that (ii) implies (i). The equivalence of (i') and (ii') is proved in the same way. □

8.8. ***Proof of Theorem 1.4****(ii)***.** By Lemma 8.7, the following lemma will complete the proof of 1.4(ii).

Lemma 8.9. *Let G be a Barsotti-Tate group of level 1 and height h over S, satisfying the hypothesis of Theorem 1.4, d be the dimension of $\mathrm{Lie}(G_s^\vee)$ over k, and $d^* = h - d$. Let H be the flat closed subgroup scheme $G^{\frac{e}{p-1}+}$, and $H^\perp = (G/H)^\vee$. Then $H^\perp$ has rank p^{d^*} over S and $\dim_k \mathrm{Lie}(H_s^\perp) \geq d^*$.*

Proof. Since H has rank p^d over S by 1.4(i), $H^\perp$ has rank p^{d^*} over S and $\dim_{\mathbb{F}_p}(G/H)(\overline{K}) = d^*$. Let $\lambda \in \mathcal{O}_{\overline{K}}$ with $v_p(\lambda) = 1/p$, and $t = 1 - 1/p$. The canonical projection $G \to G/H$ induces an injective homomorphism

$$\mathrm{Hom}_{\overline{S}}(\overline{G}/\overline{H}, G_\lambda) \to \mathrm{Hom}_{\overline{S}}(\overline{G}, G_\lambda). \tag{8.9.1}$$

By Theorem 1.6, $H^\perp(\overline{K})^{[\frac{e}{p}]} = \mathrm{Hom}_{\overline{S}}(\overline{G}/\overline{H}, G_\lambda)$ is orthogonal to $(G/H)^{\frac{e}{p-1}+}(\overline{K})$ under the perfect pairing $(G/H)(\overline{K}) \times H^\perp(\overline{K}) \to \mu_p(\overline{K})$. As $H = G^{\frac{e}{p-1}+}$, Prop. 2.8(ii) implies that the group scheme $(G/H)^{\frac{e}{p-1}+}$ is trivial. Hence we have

$$\dim_{\mathbb{F}_p} \mathrm{Hom}_{\overline{S}}(\overline{G}/\overline{H}, G_\lambda) = \dim_{\mathbb{F}_p} H^\perp(\overline{K}) = d^* = \dim_{\mathbb{F}_p} \mathrm{Hom}_{\overline{S}}(\overline{G}, G_\lambda),$$

and the canonical map (8.9.1) is an isomorphism. By the functoriality of Φ_G (8.4.1), we have a commutative diagram

$$\begin{tikzcd} \mathrm{Hom}_{\overline{S}}(\overline{G}/\overline{H}, G_\lambda) \arrow[r, equal] \arrow[d, "\Phi_{G/H}"] & \mathrm{Hom}_{\overline{S}}(\overline{G}, G_\lambda) \arrow[d, "\Phi_G"] \\ \mathrm{Lie}(\overline{H}_t^\perp) \arrow[r] & \mathrm{Lie}(\overline{G}_t^\vee) \end{tikzcd} \tag{8.9.2}$$

where the lower row is an injective homomorphism of $\mathcal{O}_{\overline{S}_t}$-modules. Put $N_0 = \mathrm{Hom}_{\overline{S}}(\overline{G}, G_\lambda)$, $M = \mathrm{Lie}(\overline{G}_1^\vee)$ and $M_t = \mathrm{Lie}(\overline{G}_1^\vee) \otimes_{\mathcal{O}_{\overline{S}_1}} \mathcal{O}_{\overline{S}_t} = \mathrm{Lie}(\overline{G}_t^\vee)$. By 8.5(ii), N_0 is identified with the kernel

of $\mathrm{F} - a(\lambda) : M_t \to M$. Let N be the $\mathcal{O}_{\overline{K}}$-submodule of M_t generated by N_0. Applying 3.12(ii) to the morphism $\mathrm{F} - a(\lambda)$, we get

$$\dim_{\overline{k}}(N/\mathfrak{m}_{\overline{K}}N) = \dim_{\mathbb{F}_p} N_0 = d^*.$$

By (8.9.2), N is contained in $M' = \mathrm{Lie}(\overline{H}_t^{\perp}) \subset M$. By applying Lemma 8.10 (ii) below to $N \subset M'$, we obtain

$$d^* = \dim_{\overline{k}}(N/\mathfrak{m}_{\overline{K}}N) \leq \dim_{\overline{k}}(M'/\mathfrak{m}_{\overline{K}}M'). \tag{8.9.3}$$

Let $\omega_{\overline{H}_t^{\perp}}$ be the module of invariant differentials of $\overline{H}_t^{\perp}$ over $\mathcal{O}_{\overline{S}_t}$. Then we have $\omega_{H_{\overline{s}}^{\perp}} = \omega_{\overline{H}_t^{\perp}} \otimes_{\mathcal{O}_{\overline{S}_t}} \overline{k}$ and

$$M' = \mathrm{Lie}(\overline{H}_t^{\perp}) = \mathrm{Hom}_{\mathcal{O}_{\overline{S}_t}}(\omega_{\overline{H}_t^{\perp}}, \mathcal{O}_{\overline{S}_t}).$$

Applying Lemma 8.10 (i) to $\omega_{\overline{H}_t^{\perp}}$, we obtain

$$\dim_{\overline{k}}(M'/\mathfrak{m}_{\overline{K}}M') = \dim_{\overline{k}} \omega_{H_{\overline{s}}^{\perp}}. \tag{8.9.4}$$

From the relations $\mathrm{Lie}(H_s^{\perp}) \otimes_k \overline{k} = \mathrm{Lie}(H_{\overline{s}}^{\perp}) = \mathrm{Hom}_{\overline{k}}(\omega_{H_{\overline{s}}^{\perp}}, \overline{k})$, we deduce

$$\dim_{\overline{k}} \omega_{H_{\overline{s}}^{\perp}} = \dim_k \mathrm{Lie}(H_s^{\perp}). \tag{8.9.5}$$

The desired inequality $\dim_k \mathrm{Lie}(H_s^{\perp}) \geq d^*$ then follows from (8.9.3), (8.9.4) and (8.9.5). $\square$

Lemma 8.10. *Let t be a positive rational number, M be an $\mathcal{O}_{\overline{S}_t}$-module of finite presentation.*

(i) *Put $M^* = \mathrm{Hom}_{\mathcal{O}_{\overline{S}_t}}(M, \mathcal{O}_{\overline{S}_t})$. Then we have $\dim_{\overline{k}}(M^*/\mathfrak{m}_{\overline{K}}M^*) = \dim_{\overline{k}}(M/\mathfrak{m}_{\overline{K}}M)$.*

(ii) *If N is a finitely presented $\mathcal{O}_{\overline{S}_t}$-submodule of M, then $\dim_{\overline{k}}(N/\mathfrak{m}_{\overline{K}}N) \leq \dim_{\overline{k}}(M/\mathfrak{m}_{\overline{K}}M)$.*

Proof. Since M is of finite presentation, up to replacing K by a finite extension, we may assume that there exists a positive integer n and a finitely generated $\mathcal{O}_K/\pi^n\mathcal{O}_K$-module M_0, where π is a uniformizer of $\mathcal{O}_K$, such that $\mathcal{O}_{\overline{S}_t} = \mathcal{O}_{\overline{K}}/\pi^n\mathcal{O}_{\overline{K}}$ and $M = M_0 \otimes_{\mathcal{O}_K} \mathcal{O}_{\overline{K}}$. Note that there exist integers $0 < a_1 \leq \cdots a_r \leq n$ such that we have an exact sequence of $\mathcal{O}_K$-modules

$$0 \to \mathcal{O}_K^r \xrightarrow{\varphi} \mathcal{O}_K^r \to M_0 \to 0, \tag{8.10.1}$$

where φ is given by $(x_i)_{1\leq i\leq r} \mapsto (\pi^{a_i}x_i)_{1\leq i\leq r}$. In order to prove (i), it suffices to verify that $\dim_k(M_0^*/\pi M_0^*) = \dim_k(M_0/\pi M_0)$, where $M_0^* = \mathrm{Hom}_{\mathcal{O}_K}(M_0, \mathcal{O}_K/\pi^n\mathcal{O}_K)$. Let

$$(\mathcal{O}_K/\pi^n\mathcal{O}_K)^r \xrightarrow{\varphi_n} (\mathcal{O}_K/\pi^n\mathcal{O}_K)^r \to M_0 \to 0$$

be the reduction of (8.10.1) modulo π^n. Applying the functor $\mathrm{Hom}_{\mathcal{O}_K}(\_, \mathcal{O}_K/\pi^n\mathcal{O}_K)$ to the above exact sequence, we get

$$0 \to M_0 \to (\mathcal{O}_K/\pi^n\mathcal{O}_K)^r \xrightarrow{\varphi_n^*} (\mathcal{O}_K/\pi^n\mathcal{O}_K)^r$$

with $\varphi_n^* = \varphi_n$. Hence M_0^* is isomorphic to the submodule $\oplus_{i=1}^r(\pi^{n-a_i}\mathcal{O}_K/\pi^n\mathcal{O}_K)$ of $(\mathcal{O}_K/\pi^n\mathcal{O}_K)^r$, and we have

$$\dim_k(M_0^*/\pi M_0^*) = r = \dim_k(M_0/\pi M_0).$$

For statement (ii), by the same reasoning, we may assume that there exists a finite $\mathcal{O}_K$-submodule N_0 of M_0 such that $N = N_0 \otimes_{\mathcal{O}_K} \mathcal{O}_{\overline{K}}$.We need to prove that $\dim_k(N_0/\pi N_0) \leq \dim_k(M_0/\pi M_0)$. Let ${}_{\pi}M_0$ be the kernel of M_0 of the multiplication by π. We have an exact sequence of Artinian modules

$$0 \to {}_{\pi}M_0 \to M_0 \xrightarrow{\times\pi} M_0 \to M_0/\pi M_0 \to 0.$$

By the additivity of length of Artinian modules, we obtain $\dim_k({}_{\pi}M_0) = \dim_k(M_0/\pi M_0)$. Similarly, we have $\dim_k({}_{\pi}N_0) = \dim_k(N_0/\pi N_0)$. The assertion follows from the fact that ${}_{\pi}N_0$ is a submodule of ${}_{\pi}M_0$. □

Remark 8.11. If we could prove the exact sequence (8.5.1) without knowing *a priori* the rank of $\mathrm{Hom}_{\overline{S}}(\overline{G}, G_{\lambda})$ for $v_p(\lambda) = 1/p$, then we would get another proof of the existence of the canonical subgroup of G. Since then, by Proposition 3.12 and (8.5.1), $\mathrm{Hom}_{\overline{S}}(\overline{G}, G_{\lambda})$ has $\mathbb{F}_p$-rank d^* under the assumptions of 1.4. Then we identify it to be a subgroup of $G^{\vee}(\overline{K})$ by $\theta_{\lambda}(G)$ (7.3.2), and define H to be the subgroup scheme of G determined by $H(\overline{K})^{\perp} = \mathrm{Hom}_{\overline{S}}(G, G_{\lambda})$. The arguments in this section imply that H is the canonical subgroup of G. For abelian schemes, this approach is due to Andreatta-Gasbarri [3].

References

[1] A. Abbes and A. Mokrane, Sous-groupes canoniques et cycles évanescents p-adiques pour les variétés abéliennes, *Publ. Math. Inst. Hautes Étud. Sci.* **99** (2004), 117-162.

[2] A. Abbes and T. Saito, Ramification of local fields with imperfect residue fields, *Am. J. Math.* **124** (2002), 879-920.

[3] F. Andreatta and C. Gasbarri, The canonical subgroup for families of abelian varieties, *Compos. Math.* **143** (2007), 566-602.

[4] M. Artin, Algebraization of formal moduli, *Global analysis*, Univ. Tokyo Press (1969), 21-71.

[5] F. Berthelot, L. Breen and W. Messing, *Théorie de Dieudonné Cristalline II*, LNM **930**, Springer-Verlag, (1982).

[6] S. Bloch and K. Kato, p-adic étale cohomology, *Publ. Math. Inst. Hautes Étud. Sci.* **63** (1986), 107-152.

[7] B. Conrad, Higher-level canonical subgroups in abelian varieties, Preprint (2005).

[8] M. Demazure, Bidualité des schémas abéliens, in *Séminaire de géométrie algébrique*, Orsay, (1967-1968).

[9] B. Dwork, p-adic cycles, *Publ. Math. Inst. Hautes Étud. Sci.* **37** (1969), 27-115.

[10] G. Faltings and L. Chai, *Degeneration of abelian varieties*, Springer-Verlag (1990).

[11] A. Grothendieck, Le groupe de Brauer III, in *Dix exposés sur la cohomologie des schémas*, North-Holland (1968).

[12] L. Illusie, Déformations de groupes de Barsotti-Tate (d'après A. Grothendieck), *Astérisque* **127** (1985), 151-198.

[13] K. Kato, On p-adic vanishing cycles (Applications of ideas of Fontaine-Messing), *Adv. Stud. Pure Math.*, **10** (1987), 207-251.

[14] N. Katz, p-adic properties of modular schemes and modular forms, in *Modular functions of one variable III*, LNM **350**, Springer-Verlag, (1973).

[15] M. Kisin and K. F. Lai, Overconvergent Hilbert modular forms, *Amer. J. of Math.* **127** (2005), 735-783.

[16] J. Lubin, Finite subgroups and isogenies of one-parameter formal groups, *Ann. of Math.* **85**, 2nd series (1967), 296-302.

[17] B. Mazur and W. Messing, *Universal extensions and one dimensional crystalline cohomology*, LNM **370**, Springer-Verlag, (1974).

[18] D. Mumford, *Geometric invariant theory*, Springer-Verlag, (1965).

[19] M. Raynaud, Spécilisation du foncteur de Picard, *Publ. Math. Inst. Hautes Étud. Sci.* **38** (1970), 27-76.

[20] T. Sekiguchi, F. Oort and N. Suwa, On the deformation of Artin-Schreier to Kummer, *Ann. Sci. de l'É.N.S.* 4^e série, tome 22, No.3 (1989), 345-375.

[21] J. Tate and F. Oort, Group schemes of prime order, *Ann. Sci. de l'É.N.S.* 4^e série, tome 3, No. 1 (1970), 1-21.

LAGA, Institut Galilée, Université Paris 13, 93430 Villetaneuse, France

E-mail address: tian@math.univ-paris13.fr